Blundells Hill Golf Club Limited

Staff Handbook

Issue:	Date:	Description of Amendment:	Authorised by:
00	January 2008	Original	Steve McKie
01	October 2008	General Review inc change of discipline procedure	Steve McKie
02	February 2018	General Review	Steve McKie
03	December 2021	General Review	Steve McKie

CONTENTS

Section: Subject:

15 COMPANY RULES

Introduction - Disciplinary Rules – Behaviour at Work - Company Property - Company Vehicles - Health and Safety – Timekeeping / Absence - Working Standards - Computer Software and Equipment - Rules Covering Gross Misconduct

16 DISCIPLINARY PROCEDURES

Disciplinary Procedure - Breaches of Disciplinary Rules - Gross Misconduct - Offences other than Gross Misconduct - Stages of Warning – Stage 1: Informal Verbal Warning by Supervisor - Stage 2: Verbal Warning by Supervisor - Stage 3: Formal Warning by Director - Stage 4: Suspension without Pay - Stage 5: Dismissal - Validity of Warnings - Disciplinary Appeals - Appeals against Dismissal

17 GRIEVANCE PROCEDURE

Introduction - Stage 1: Informal discussion - Stage 2: Request a Meeting - Stage 3: Appeal to the Board

18 GDPR DATA PROTECTION POLICY

Objective - Eight principles - Consent to the Company holding personal information

19 USE OF COMPANY COMPUTER POLICY

Scope – Objective – Policy - Portable Computers (Laptops)

20 SOCAIL MEDIA POLICY

21 CCTV POLICY

22 DATA PROTECTION POLICY FOR EMPLOYEES, WORKERS & CONSULTANTS

Scope – Objective – Policy

23 ALCOHOL & DRUG POLICY

Policy **–** Aims **–** Drugs **–** Cannabis **–** Alcohol **-** Provisions

24 EQUALITY AT WORK POLICY

Commitment – Objectives - Complaints

25 DIGNITY AT WORK POLICY

Aim of the Policy – Definition – Responsibility – Support – Action – Investigation – Discipline

26 COMPANY VEHICLE POLICY

Usage – Fuel - Parking and Congestion Charges – Maintenance – Security - Incidents -

Violations and Convictions - Driving Bans - Other considerations

27 HEALTH & SAFETY POLICY

28 SMOKE-FREE POLICY

29 STRESS POLICY

Introduction - Definition of Stress – Policy – Responsibilities - Function of Safety Representatives - Role of the Safety Committee

30 QUALITY POLICY

31 ENVIRONMENT POLICY

32 GENERAL CONDITIONS OF EMPLOYMENT

Acts Prejudicial to the Company – Appraisals - Bad Weather Conditions - Bereavement Leave – Bullying - Buying or Selling of Goods – Capability - Cash Handling - Cash Handling / Petty Cash - Change of Address and Telephone Number – Collections - Company Collections - Compassionate Leave – Confidentiality - Consultants or Contractors (Private Use of) - Fire and Evacuation Procedures - First Aiders – Gambling – Gifts / Hospitality – Housekeeping - Ideas and Suggestions - Jury Service / Court Attendance – Keys - Letters of Reference - Mobile Phones - Use of Mobile Telephones when Driving - Notice Board(s) - Parking on Company Premises - Personal Mail - Employees' Property - Personal Telephone Calls - Protective Work Wear – Redundancy - Religious and Political Activities - Retirement Age - Right of Search - Secondary Employment - Short-time Working and Layoff - Socialising with Suppliers, Customers or Clients - Standards of Dress and Appearance - Statements to the Media - Territorial Army Leave - Theft / Dishonesty - Trade Unions and Collective Agreements - Training Courses - Variations to Terms and Conditions - Workplace Monitoring

33 POLICY REVIEW

1 INTRODUCTION

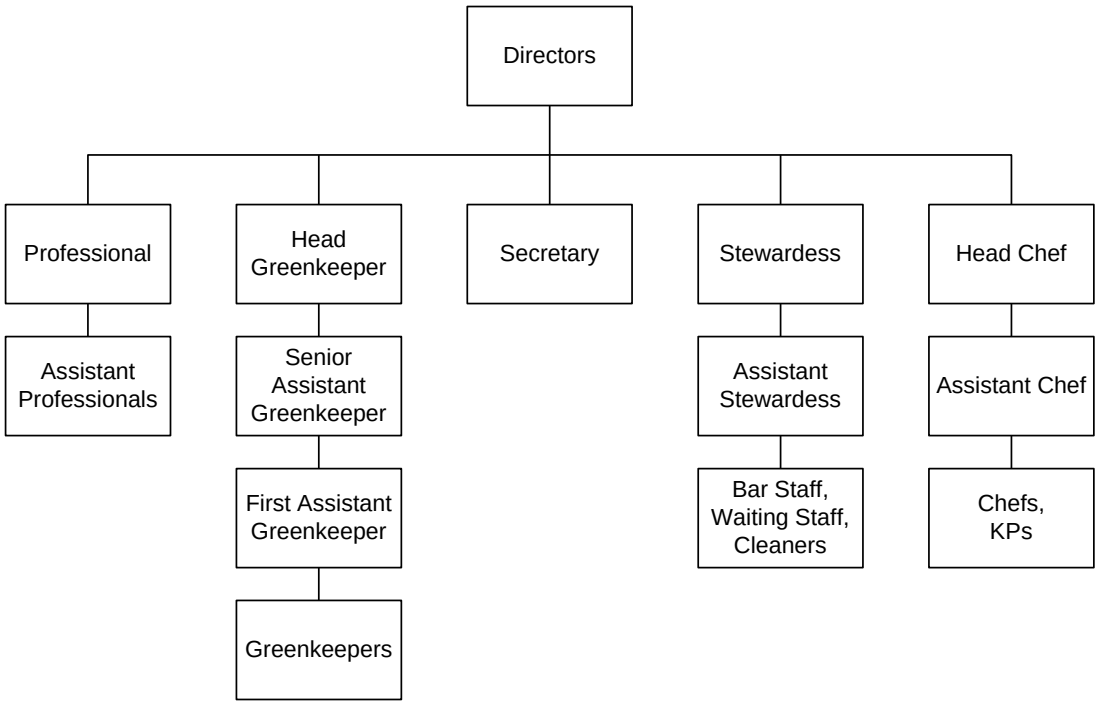
The aim of this Staff Handbook is to provide a concise and practical overview of:

- What the staff of Blundells Hill Golf Club Limited need to know about their employment.
- The Company's policies.
- What will be expected from an employee.
- What an employee may expect from the Company and their fellow employees.

Although provided in reference book format, it should be read carefully as the contents unless specified otherwise forms part of each employee's Contract of Employment. Employees are encouraged to seek help and guidance on any points about which they are not absolutely clear.

2 COMPANY ORGANISATION CHART

The following chart shows the organisation and reporting structure of the Company:



3 WAGES AND SALARIES

Bank Account Details

Upon joining Blundells Hill Golf Club Limited, each employee will be asked to provide details of a bank or building society account into which he or she wishes his or her wages or salary to be paid. If these details change the employee must inform the Club Secretary as soon as possible or payments may be delayed.

Payment

Employees will receive a payslip showing how the total amount of his or her wages or salary payment has been calculated and the deductions that have been made for Income Tax, National Insurance, Pension etc.

Wage queries (e.g. incorrect payment, shortages, error in deductions etc) should be raised with his or her Head of Department within one week of payment.

It is not the Company's practice to make loans or advances of pay.

Overpayments

Should an employee be overpaid in error, he or she must notify his or her Head of Department without delay. The total of the overpayment will normally be deducted from his or her next payment. *If this should cause hardship, arrangements may be made for the overpayment to be recovered over a longer period.*

Income Tax

At the end of each tax year, each employee will receive a P.60 Tax Form showing the total pay he or she has received from the Company during that year and the amount of deductions made. The employee should retain this document in a safe place as he or she may need to produce it when making enquiries with the Inland Revenue or DSS.

The Company's tax office and reference number are as follows:

H.M. Inspector of Taxes,
West Lancs and West Cheshire Area,
PO Box 61,
Leigh,
Lancashire,
WN7 1XZ

Reference number 709/STC422

4 HOURS OF WORK

Hours of Work

Each employee's normal hours of work are detailed in his or her Contract of Employment.

Additional Hours

There will be occasions when the Company faces staff shortages due to sickness and other absences, surges in business, the need to supply services quickly to retain customer goodwill, or to keep a competitive edge. In these circumstances there may be a need to work additional hours to those quoted in employees Contracts of Employment.

While no one will be compelled to work additional hours, it is hoped that employees will consider such requests positively to ensure that the needs of clients are met and to deliver the services expected from the business.

Overtime

Overtime premium will only be paid for hours worked in excess of 40 hours per week. Overtime premium rates payable are listed in the employee's Contract of Employment.

Hours worked in excess of normal contractual hours may be compensated by time off in lieu by mutual agreement between the employee and management.

The working of overtime will be maintained on a voluntary basis where possible but it is a condition of your employment that you are willing to do so when requested to meet the need of the business.

Absence / Timekeeping

The Company expects employees to arrive for work punctually and be ready to commence work at the appointed time at the start of each day. Employees who are unable to attend work for whatever reason (or, in exceptional circumstances, someone on their behalf) must notify the Company as soon as possible and by the start of the employee's normal duty on the first day of absence.

Lateness in attending work on more than one occasion in a week or on more than three occasions in a month will render an employee liable to disciplinary action.

Each employee's Contract of Employment will state whether he or she must personally clock or swipe in and out. Personnel using another employee's card will be deemed to be committing Gross Industrial Misconduct and will be subject to the Disciplinary Procedure.

All absences must be notified in accordance with the procedures laid down within this manual. Failure to follow such procedures will render the employee liable to disciplinary action and or loss of appropriate payment.

All other absences from work; including leaving before normal finishing time(s) will be treated as unauthorised and will render an employee liable to disciplinary action, unless express permission for the absence has been given. In severe or repeated cases of such unauthorised absence, considered to be a breach of contract, the employee will be liable to have his or her employment terminated.

Employees are required strictly to comply with any time recording procedures relating to their work.

5 TERMINATION OF EMPLOYMENT

The required notice periods for the termination of employment by the employee or by the Company are detailed in each employee's Contract of Employment. Notice to terminate employment must be given by an employee in writing to his or her Head of Department or to a Director.

If an employee fails to attend work normally during his or her notice period, this will be treated as unauthorised absence and may depending upon the circumstances be considered an act of gross misconduct.

The Company reserves the right to utilise any outstanding accrued holiday entitlement against all or part of the notice period. The right is also reserved to make a payment in lieu of notice.

During his or her notice period an employee may be requested not to attend for normal duties but must nevertheless remain available for work if required.

In the event of dismissal due to gross misconduct, the Company will terminate employment without notice.

6 PENSION SCHEME ARRANGEMENTS

If you are eligible, the Company will auto-enrol you into a pension scheme, in accordance with the Company's pension auto-enrolment obligations.

Full details of the scheme will be provided when you are enrolled, including the minimum contribution level that you will be required to make and your right to opt out if you do not want to join the scheme. While participating in the scheme, you agree to worker pension contributions being deducted from your salary.

The scheme is subject to its rules as may be amended from time to time, and the Company may replace the scheme with another pension scheme at any time.

Further details of the Scheme are available from the Club Secretary.

7 HOLIDAY ENTITLEMENT

Entitlement

Each employee's annual paid holiday entitlement is included as part of his or her Contract of Employment.

Holiday Requests

To ensure the smooth running of the Company and to safeguard staff holiday arrangements, each employee must complete a holiday request form for all annual holidays not laid down by the Company and have the request approved by a Director. Holiday requests will only be agreed if they are presented on a holiday request form and verbal notification will not be accepted.

Holidays should not be booked without prior management approval. The Company will not be held responsible for any unrecoverable deposit or other losses incurred by you as a result of a prior booked holiday which is subsequently not approved by the Company.

As much notice as possible is required, but at least 4 weeks' notice of an employee's intention to take holidays of one week or more is requested. Holidays for lesser periods require at least 2 week's notice. A limited number of half days of flexible holiday entitlement are permitted subject to appropriate approval.

Requests for more than 10 consecutive working days as holiday will only be approved in special circumstances, and strictly at management discretion based on the needs of the business. In such situations the employee should obtain provisional management approval of his or her holiday request prior to making any financial commitment.

A previous absence from work is not permitted to be subsequently taken as holiday.

Holiday Allocation

All holiday dates will be allocated on a first come, first served basis to ensure that the operational efficiency and minimum staffing levels are maintained throughout the year. If holiday times clash, the first person to book is given priority. If holiday arrangements are changed, the member of staff must accept the holiday times left available to suit the business.

Cancellations

Holiday cancellations must also be notified to the Company in writing and holidays already approved will not automatically be cancelled.

Holiday Year

The holiday year runs from 1st Jan to 31st December. Further details may be obtained from the Club Secretary.

You will not be able to carry over any unused holiday entitlement from one holiday year to another, without the written permission of a director. Any holiday not taken in the holiday year will be lost.

Public Holidays

In addition to the annual holiday entitlement, employees are allowed some customary public holidays with pay, or alternative days as decided by management. Details of these are included in each employee's Contract of Employment. However, to be entitled to payment for that day, an employee must be actually in work at the time that a customary public holiday falls due.

It is a condition of employment that an employee must be prepared to work on a customary public holiday if required to do so. Those hours that are worked will be paid at either double time or at his or her normal rate of pay with another paid day in lieu to be taken at a later agreed time. Bar staff will be paid at basic rate for a bank/public holiday (See Contract of Employment)

If an employee is absent due to sickness directly before and/or after a customary public holiday, he or she will be required to provide a doctor's certificate or, if the absence is not due to sickness, proof of other serious and unavoidable domestic emergency. Failure to do so will result in non-payment for the holiday.

Customary public holidays (including statutory and bank holidays) falling within periods of annual leave are not to be added on at the end of the period or taken separately without prior approval. Should a bank holiday fall during an employee's holiday he or she is not automatically to take the following day off without obtaining prior permission from his or her Head of Department.

Club Secretary and Green Keeping Staff

The Club Secretary and Green Keeping staff are required to reserve part of their holiday entitlement to cover the fixed days over the Christmas/New Year period. The Company will publish a notice as early as possible in the year to advise you how many days of the above entitlement should be reserved.

Religious Holidays

Those members of staff wishing to observe religious holidays are permitted to do so from within the overall holiday entitlement. Proposed absence due to a religious festival must be subject to the staffing needs of the Company permitting that day to be taken.

Start of Employment

In the first year of employment holidays may not be taken in advance of the amount accrued unless prior approval has been obtained. If an employee has

insufficient accrued or holiday pay at the time of a fixed holiday, those days will not have an entitlement to pay.

Where an employee has a previously booked holiday that requires time off from work during the first 13 weeks of employment, the right is reserved to extend his or her probationary period by a time equivalent to the holiday absence.

End of Employment

In the event of termination of employment, any holidays earned but not taken in that year will be paid for. Personnel leaving employment during a holiday year will be paid on a pro rata basis for each complete calendar month of service during the year. However, in the event of an employee having taken holidays that have not been earned pro rata in the holiday year, then the appropriate payments will be deducted from his or her final wage / salary.

8 MEDICAL, SICKNESS AND SICK PAY PROCEDURES

Medical Appointments, etc.

As far as possible all appointments with doctors, dentists, opticians, etc. should be made outside normal working hours. Where this is impracticable, appointments may be made during working hours and wherever possible with the prior permission of the employee's Manager.

Whilst there is no entitlement to payment for such absences, employees would normally be expected to make the time up. Absence without permission to attend appointments may be regarded as unauthorised absence, which may result in disciplinary action.

It is in each employee's own interest to be registered with a Doctor or Dentist whose surgeries are near their home or work.

Payment

If an employee is absent from work due to personal sickness or injury, the Company is only responsible for paying Statutory Sick Pay (SSP) if the employee qualifies and complies with the rules set out below and in the following section 9. To qualify for payment of SSP the employee must comply with all the requirements, otherwise he or she will not receive payment or payment may be delayed. In some circumstances failure to abide by the requirements may also lead to disciplinary action being taken.

Staff may have their wages made up to normal pay at the absolute and sole discretion of the Directors.

First day of absence

An employee unable to attend work due to sickness must contact his or her Head of Department or the Club Secretary within one hour of the employees normal start time on the first working day of absence and state:-

- The reason for the absence
- The date when he or she first became ill (including weekends, days-off, holidays, bank holidays etc).
- The last date he or she worked.
- The date he or she expects to return to work, or if not known, the best estimate.

Such notification is to be made personally or, if the employee is unable to do so personally, by a relative, neighbour or friend)

Absences of not more than 7 calendar days

On each subsequent day of absence after the first day the employee must telephone his or her Supervisor / Manager before midday to report on progress towards a return to work. If the employer does not receive notification, the absence will be classified as 'unauthorised'.

On return to work after any absence of up to 7 CALENDAR DAYS the employee is required to complete a Sickness Self-Certification Form, available from the Club Secretary. This Form must be handed to his or her Head of Department for signature.

Absences of more than one week

If the absence is likely to continue for more than one week, the employee must request the Company to send you a Self-Certification form, which should be fully completed and returned to the Company to arrive by the fourth working day of absence. This Self-Certification will cover absence for the first 7 calendar days. After one week the employee is required to provide Medical Certificates at regular intervals for the entire period of sickness absence.

The employee is required to telephone the Company on a weekly basis to keep it informed of progress and the anticipated length of absence.

Contact with Infectious Diseases

If an employee is prevented from attending work because of contact with an infectious disease, he or she should still follow the above reporting procedure. The employee will be entitled to receive full pay less any benefits payable under SSP and his or her period of absence on this account shall not be reckoned against entitlement to normal sick leave.

In the case of contact with other infectious or contagious diseases that do not prevent an employee from working, he or she should not stay away from work

unless feeling unwell but should report the fact of contact to his or her line Manager.

Return to work Interviews

Wherever possible, and as soon as possible, the Company will aim to carry out a Return to Work(ing) interview to discuss:

- How the returning employee is feeling.
- His or her absence.
- How, if at all, the Company can aid the return to work and, if applicable
- The Company's expectations for future attendance.

Medical examinations

If the Company considers it necessary, arrangements will be made for an employee to be medically examined. The Company reserves the right to require employees to receive a medical examination by the Company Doctor. If an employee is medically examined a copy of the report can be sent to his or her own Doctor in addition to being supplied to the Company. The Company will only seek information from an employee's General Practitioner about the state of the employee's health when that information is considered essential for employment purposes. Where applicable, employees will be fully informed of their rights of access to any such reports.

False Statements

To make a deliberately false or misleading statement in respect of sickness absence is misconduct and may lead to dismissal in accordance with the Company's disciplinary rules and procedures.

9 STATUTORY SICK PAY

Employees are entitled to SSP during absence due to personal sickness or injury providing they follow the Company's absence reporting procedure and providing they are not in one of the excluded categories listed below.

SSP will only be paid for whole days of incapacity for work. Incapacity is when an employee is unable to attend work on a contractual working day because he or she has a specific disease or is physically or mentally disabled from doing so.

There are certain categories of employees who are not entitled to SSP. An employee will not qualify for SSP if he or she:

(a) Has average weekly earnings of less than the lower earnings limit for National Insurance contributions liability.

(b) Has claimed certain State benefits within the previous 56 days e.g. job seekers allowance, maternity allowance, incapacity/sickness benefit.

(c) Has gone sick during a stoppage of work at his or her place of employment due to a trade dispute and has taken part in that dispute.

(d) Is in legal custody.

Expectant mothers are disqualified from SSP for the period during which Statutory Maternity Pay is paid.

The Company is liable to pay an employee SSP for 28 weeks in a linked or unlinked period of incapacity for work. Once the 28 weeks have been exhausted the sick pay liability transfers to the Department of Social Security.

Payment of SSP will only be made on those days when an employee is normally contracted to work. These are known as "Qualifying Days".

SSP will only be paid from the fourth qualifying day of absence, the first three being "waiting days". These do not have to be served again to qualify for SSP if the next Period of Incapacity for Work falls within 56 days.
To obtain SSP the Company's rules on absence reporting and recording must be followed. The Company has the right not to pay SSP if it feels that an employee was not genuinely incapacitated. The Company may ask the Inland Revenue to investigate where it feels that an employee's self-certification absences are not genuine.

Payment of SSP will be through the normal payroll procedure and will be subject to the normal deductions.

The Company reserves the right to withhold a payment of SSP if:

i Sickness notification is made late.
ii Evidence of incapacity is not produced.
iii Evidence of incapacity is not satisfactory.

If SSP is withheld for any reason, the employee has the right to request a written statement explaining the days which are to be paid, including the amount of SSP and the reasons for not paying SSP on the other days.

However the period for which payment is withheld does not reduce the employee's SSP period of entitlement and is not counted as waiting days.

If an employee does not agree with the Company's decision to withhold any SSP payments, he or she has the right to lodge a complaint with the local office of the Inland Revenue. They will investigate the matter and make a finding either in the employee's favour or uphold the Company's decision. If they find in the employee's favour then the Company will be obliged to pay to the employee any unpaid SSP entitlement.

10 MATERNITY LEAVE, ADOPTION, PAYMENTS, PROCEDURES AND CONDITIONS

Employees expecting a baby have the statutory right to take reasonable paid time off work for antenatal care. The right does not depend on any minimum service qualification. There is however an expectation that every effort should be made by the employee to minimise the disruption created by her absences.

Other than for the first appointment, the employee must, if requested, produce a certificate confirming that she is pregnant and an appointment card (or similar document) showing that an appointment has been made.

Maternity Leave

Expectant mothers are entitled to Maternity Leave of up to 52 weeks regardless of length of service or hours of work. This is made up of 26 week's Ordinary Maternity Leave immediately followed by 26 weeks' Additional Maternity Leave.

Notification Requirements

To qualify for Maternity Leave from work the employee must provide certain information.

1. By the 15th week before the expected week of confinement (EWC) the employee must provide written notification of her pregnancy, giving the date of the expected week of confinement, when she wants her maternity leave to start.
2. The employee can change her mind about when she wants to start her leave providing she gives at least 28 days' advance notice.
3. The employee must provide evidence of the expected date of confinement. This must be in the form of a Certificate of Expected Confinement (Form MATB1) issued by a Doctor or Midwife. Note however that this will not be issued earlier than 14 weeks before the expected date of confinement.
4. Immediate notification must be made if the employee is taken into legal custody or starts work for another employer during her Maternity Pay Period (MPP).
5. If an employee gives birth before proper notification has been made or before the date already given, her Maternity Leave and Pay starts automatically on the date of birth and she must without delay provide notification of the date of birth in writing.
6. An employee who is absent from work due to illness will normally be able to take sick leave until she starts maternity leave on the date notified to her employer. However, if the illness is related to her pregnancy, the maternity leave period starts automatically on the day after the first day of absence following the beginning of the fourth week before the expected week of

childbirth. The employee must, as soon as reasonably practicable, provide written notification of the reason for her absence.

Failure to abide by all the notification requirements, or if an employee is late in doing so without good reason, may result in the loss of Statutory Maternity Pay.

Statutory Maternity Pay (SMP)

Statutory Maternity Pay is paid for a period of 39 weeks as follows:

The first six weeks are paid at 90% of the employee's average weekly earnings calculated from the 8 week period up to and including the qualifying week. The remaining weeks are paid at a rate set by the Government and reviewed annually.

In the event of an employee's average earnings being below the set rate, then 90% of her average weekly earnings will be paid throughout the whole of the Maternity Pay Period (MPP), which is a maximum of 39 weeks.

An employee will be entitled to Statutory Maternity Pay providing she satisfies all of the following conditions.

a. Has been in the Company's employment for at least 26 continuous weeks (irrespective of the number of hours worked) ending with the qualifying week, that is the 15th week before the baby is due, and has average weekly earnings at that time of not less than the lower earnings level for the payment of NI contributions.

b. Is still pregnant at the 11th week before the baby is due, or has already been confined.

c. Has provided written notice of her Maternity Leave and has stopped work.

Details of the amount of payment due, and how the payments are made, are available on request.

Return to Work

Providing she meets the requirements, an employee on Ordinary Maternity Leave has the right to return within 26 weeks to the same job, on the same terms and conditions, as if she had not been away.

An employee on Additional Maternity Leave is entitled to return, by the end of the twenty sixth week after that leave starts, to the same job or, if this is not reasonably practicable, to a suitable alternative.

An employee is not expected to give prior notice if she intends to return to work immediately after the end of her maternity leave period. However if she intends to return to work BEFORE the end of the Maternity Leave entitlement she **must** give at least 8 weeks' notice of her intended return. The Company reserves the right to postpone her early return for up to 8 weeks' if she fails to give the appropriate notice.

If an employee is unable to return to work on the due date because she is sick, she must comply with the absence procedure shown earlier in this Handbook.

Employees have no statutory right to return to work on different terms and conditions.

Keeping in Touch Days

The Company may make reasonable contact with the employee (and vice-versa) while she is on maternity leave to discuss a range of issues including her plans for returning to work or to keep her informed of important developments at the workplace.

Furthermore, she may attend work for up to 10 Keeping In Touch Days. This can only be undertaken by agreement at any stage of her Maternity Leave (with the exception of the first 2 weeks after the baby is born) and her SMP will continue to be paid.

ADOPTION LEAVE

If you adopt a child provided that you fulfil the required criteria you may be eligible for the following rights:

- 52 weeks of statutory adoption leave.
- Statutory Adoption Pay for up to 39 weeks of the leave.

Further details should be obtained from The Club Secretary.

11 PARENTAL LEAVE PROCEDURES AND CONDITIONS

All eligible employees who have a child under the age of eighteen have the statutory right to take Parental Leave. This leave is only for looking after the welfare of their child and can include making arrangements for the good of their child.

Entitlement to Leave

Providing the employee meets the qualification requirements described below, his or her entitlement is up to 18 weeks unpaid leave for each child. To qualify for Parental Leave the employee must have one year's continuous service on the date he or she wishes the leave to start and he or she must either:

1. Be the parent (named on the birth certificate).
2. Have legally adopted a child under the age of 18.
3. Have acquired formal parental responsibility for a child under eighteen years.

Procedures and Conditions

An employee wishing to take Parental Leave must comply with the following conditions:

a. The employee is not permitted to take leave in blocks of less than one week. If he or she takes odd days, they will count as one week from the entitlement. An exception to this rule applies only if the child is disabled, in which case the employee is permitted to take leave in multiples of one day.

b. The employee may be permitted to take more than one week's leave at a time, up to a maximum of 4 weeks in a year.

c. The employee must make a written request at least 21 days before the date on which he or she wishes to commence the leave.

d. The employee will be required to provide evidence to support the request for leave.

e. The employee must stipulate the exact date on which he or she wishes the leave to begin, unless he is a father wishing to take leave straight after the baby is born, or he or she is a prospective adoptive parent wishing to take leave straight after the child is placed with him / her for adoption. In such cases the notice required must:

- Specify the expected week of child birth or adoption.
- Specify the leave duration.
- Be submitted at least 21 days before the child birth week or adoption placement.

f. Where the Company's business will be adversely affected, the leave may be postponed for up to 6 months from the date the employee wished to start leave and a suitable time will be agreed when the leave can be taken within that six month period. However, leave may not be postponed immediately after the birth/adoption of the child.

g. If an employee is found to have dishonestly taken Parental Leave then he or she will be liable to serious disciplinary action, which may include the termination of employment.

Return to Work

After taking Parental Leave for a period of 4 weeks or less the employee is entitled to return to the same job. If a longer period of leave is agreed the employee is entitled to return to the same job, or if that is not possible, a job which has the same or better terms and conditions as the old job.

SHARED PARENTAL LEAVE POLICY

The right to shared parental leave and statutory shared parental pay enables eligible employees who are parents (whether by birth or adoption) to take paid and/or unpaid leave within the first year of their child's life or the first year after their child's placement for adoption, provided always that the eligible mother or adopter has volunteered to end their maternity leave and/or pay or adoption leave and/or pay early (or has already returned to work early). Eligibility and pay are in accordance with the current statutory provisions. You should notify your Line Manager at an early stage of your needs so that your entitlements and obligations can be explained to you.

12 PATERNITY LEAVE AND PAY

Prospective fathers have the right to take one or two weeks' paid paternity leave in the 8 weeks following the birth of a child. The leave has the purpose of caring for the child or supporting the child's mother.

To qualify for leave and statutory paternity pay an employee must:

- Have completed 26 weeks of continuous service by the beginning of the 15th week before the expected week of child birth (EWC).
- Be the father of the child, or be married to or the partner of the child's mother.
- Have responsibility for the upbringing of the child.

Notification that an employee wishes to take leave must be given under the same qualifying conditions (i.e. 15 weeks before the EWC). When making notification the employee must state the EWC, the leave commencement date and the amount of leave requested. If the planned date of leave commencement changes for any reason, a full 28 days written notice of the new date should be given unless it is not reasonably practicable to do so.

The rate of statutory paternity pay is that laid down by statute and is normally reviewed annually.

13 TIME OFF FOR DEPENDANTS

Employees are entitled to take reasonable unpaid time off to deal with incidents involving a 'dependant'. A 'dependant' is defined as the employee's parent, wife, husband, partner, child or someone who lives as part of the family, for example somebody for whom the employee is responsible. Leave taken under this entitlement is intended to cover unforeseen matters and the amount of leave will

be one or two days at the most. The time off should be limited to the minimum required to make arrangements for care and not for the provision of care itself.

An employee has the right to time off in the following circumstances:

a. To help with a dependant who falls ill or is injured.
b. To cope when the arrangements for caring for a dependant unexpectedly break down.
c. To make longer term care arrangements for a dependant who is ill or injured.
d. When a dependant gives birth.
e. When a dependant dies.
f. To deal with an unexpected incident concerning a dependant during school hours.

In the first three cases the dependant can be someone who relies on the employee in the particular emergency.

When making a request for time off the employee must give as much notice as is reasonably practicable in the circumstances. If the employee is found to have dishonestly taken such time off then he or she will be liable to serious disciplinary action.

If the employee knows in advance that he or she is going to require time off to deal with a matter involving a dependant, the employee should arrange to take this time as holiday subject to the availability of outstanding flexible annual leave entitlement, or in circumstances which involve a child he or she may be entitled to take Parental Leave.

14 FLEXIBLE WORKING PROCEDURES AND CONDITIONS

Flexible Working

In the interest of operational efficiency employees may be required to transfer to alternative work, and it is a condition of employment that they are willing to do so when requested.

Employee Request for Flexible Working

An employee who has at least 26 weeks' continuous service at the date an application is made, has the right to make a request to work flexibly providing he or she meets the necessary qualifying criteria and conditions shown below:

Conditions

You must not have made another application to work flexibly during the past 12 months.

Applications and Procedure

An employee's application to work flexibly may not always involve a significant change to his or her current working hours or pattern. However, if a request is made and if such an application is accepted, it will mean unless agreed otherwise a permanent change to the employee's contract of employment.

In the event of an application being made the regulations provide a procedure which must be followed. A summary of the procedure is shown below:

(a) The employee must make a written application to a Director. However, before making such an application he or she must have considered the effects it would have on the business and explain how these might be accommodated. Where a drop in working hours is being requested the employee should also have considered the subsequent financial implications upon himself / herself.

(b) A meeting will be arranged with the employee to discuss the application. The employee may bring a fellow employee to the meeting if he or she wishes. The companion may be the workplace TU representative if this applies.

(c) The employee will receive a written response following the meeting, either to agree a new work pattern and confirm a start date or to reject the application.

If the application is rejected the employee will be given clear business reasons as to why the application has been rejected and the reasons why such grounds apply in the circumstances. Such reasons may include extra costs, detrimental effects on the business, inability to reorganise work amongst other staff, recruitment of extra staff, lack of work during the proposed working periods or planned work structural changes.

(d) The employee has the right to appeal against a decision to reject his or her application.

(e) The Company will be complete the application to work flexibly within 3 months.

15 COMPANY RULES

Introduction

In any organisation it is necessary to have rules in the interests of both the employer and employees. The rules set standards of performance and conduct at work, while the Disciplinary Procedure helps to ensure that the standards are adhered to and provides a fair method of dealing with alleged failure to observe them. Both are designed to help promote fairness and order in the treatment of individuals and in the conduct of industrial relations.

It is important that all employees know what standards of conduct are expected of them. The rules should be seen not as sanctions. They are designed to emphasise and encourage improvements in an individual's conduct.

Every effort will be made to ensure that any action taken under the Disciplinary Procedure will be fair, with the employee concerned being given the opportunity to state his or her case and appeal against any decision he or she considers to be unjust.

The following procedure should ensure that:

- All employees are fully aware of the standards of performance, action and behaviour required of them.
- Disciplinary action, where necessary, is taken speedily and in a fair, uniform and consistent manner.
- An employee will only be the subject of disciplinary action after careful investigation of the facts and the opportunity to present his/her side of the case.

Disciplinary Rules

It is not practicable to specify all disciplinary rules or offences which may result in disciplinary action, as circumstances may vary depending on the nature of the work and the misconduct. Even a minor infraction may be treated as serious misconduct depending on the circumstances that may apply at the time.

Failure to comply with the following general rules will render an employee liable to disciplinary action and, where no improvement is forthcoming, possible dismissal. This list is not exhaustive:

1 Behaviour at Work

1.1 Employees should behave with civility at all times and rudeness will not be tolerated towards clients, members of the public or fellow work colleagues. Objectionable, insulting or offensive behaviour or excessive bad language will render an employee liable to disciplinary action.

1.2 Employees must use their best endeavours to promote the interests of the Company and shall, during your normal working hours, devote the whole of their time, attention and abilities to its business and affairs.

1.3 Any involvement in activities which could be construed as being in competition with the Company is forbidden.

1.4 Activities which result in adverse publicity to the Company, or which cause it to lose faith in an employee's integrity, may give the Company grounds to take disciplinary action. This applies to the employee's activities outside working hours as well as during working time (including time whilst away from his or her normal place of work).

1.5 An employee shall not during, or after the termination of, his or her employment, disclose to any person whomsoever any confidential information regarding the Company, its business or trade secrets.

1.6 All reasonable instructions from an employee's manager / supervisor are to be obeyed.

1.7 Unauthorised personal use of the business telephone is a disciplinary offence.

1.8 Any occasion when an employee is found to be asleep at work will be treated as a serious breach of the rules.

1.9 Employees are reminded that they are paid to work on Company business and are not allowed to buy or sell goods on their own behalf on Company premises.

2 Company Property

2.1 Use of Company property for any purpose other than normally defined duties is not permitted.

2.2 Unless required for business purposes, Company property of any type is not to be taken away from the premises except with prior approval.

2.3 Employees must immediately notify the appropriate member of management of any damage to property or premises, whether belonging to the Company or a client.

2.4 Employees are responsible for the care and safe keeping of any tools, equipment or clothing provided by the Company. The Company reserves the right to charge for any items that are unaccountably lost or damaged by an employee, or stolen as a result of an employee's negligence. Any such deduction will be made through the payroll after notice has been given by the Company of its intention.

3 Company Vehicles

Only authorised members of staff may drive the Company's vehicles. See the Company Vehicle Policy for rules regarding their use.

4 Health and Safety

4.1 The Company will do all in its power to ensure the well being and safety of all its employees. Any action by an employee that endangers the health or safety of himself / herself, other employees or other persons, will lead to disciplinary action being taken and could result in dismissal.

4.2 Employees must abide by the general health and safety rules and procedures at all times.

4.3 All accidents, no matter how slight, whether involving an employee or

member of the public, must be reported and entered into the Accident Book. False statements or deliberate interference with evidence following an accident or dangerous occurrence is a serious offence.

4.4 Each employee should make himself / herself familiar with the Company's Health and Safety Policy and his or her own health and safety duties and responsibilities, as contained within this manual.

4.5 Each employee must report any potential hazard or unsafe conditions to his or her Head of Department.

4.6 Any personal electrical appliance brought on to the Company premises by an employee must be battery powered because the Company is not prepared to inspect, service and certify personal appliances in order to comply with the Electricity At Work Regulations 1989.

5 Timekeeping/Absence

5.1 Employees are expected to attend for work punctually at the specified time(s). Persistent or excessive lateness in attending work will be liable to disciplinary action.

5.2 Employees may not leave work prior to their normal finishing time without permission. If an employee requires time away from work during normal working hours, providing the request has been granted, he or she must report upon leaving and returning to work as appropriate.

5.3 All absences must be notified in accordance with the procedures laid down earlier in this Handbook.

5.4 Absence for any reason must be notified as soon as possible, preferably by telephone on the first day of absence. It is an employee's responsibility to keep the Company advised of the circumstances that are preventing him / her from attending work, and also the likely date of his or her return.

5.5 Employees are required to comply strictly with any time recording/reporting procedures relating to their area of work. Failure to follow the time recording and absence reporting procedures will render an employee liable to disciplinary action.

IMPORTANT: Employees should be aware that any period of unauthorised absence is a breach of contract.

6 Working Standards

6.1 Unsatisfactory standards (i.e. quality) of work will be investigated and employees concerned will be subject to disciplinary action if poor job performance is proved to have been caused by carelessness or neglect of duty.

6.2 Unsatisfactory output (i.e. work rate) will be viewed similarly to the above and may result in action being taken to remedy the employee's deficiencies, or to enforce the disciplinary procedure if improved output is not maintained.

6.3 All employees are responsible for the cleaning up of any mess or spillage, however caused, without delay or discussion (excluding offensive/harmful waste which must be dealt with under local disinfection/decontamination rules by a trained person wearing appropriate protective equipment). If there is any doubt, employees should seek guidance from their Head of Department.

7 Rules Covering Gross Misconduct

Offences under this heading are so serious that an employee who commits them will normally be summarily dismissed, regardless of whether there are any active warnings on their record. In such cases, the Company reserves the right to dismiss without notice of termination or payment in lieu of notice. Examples of gross misconduct include:

- any breach of the criminal law, such as theft
- any unauthorised possession or removal of Company products or property, or property belonging to another employee, client, customer or visitor, fraud (including making fraudulent or false expense claims), deliberate falsification of records, false declarations in connection with employment or applications for employment or any other form of dishonesty
- using the Company's property, materials or equipment to carry out work for third parties on a personal basis without permission
- misuse of Company benefits, such as improper use of a staff discount card
- offering, promising or giving a bribe or requesting, agreeing to receive or accepting a bribe or bribing a foreign public official in connection with employment contrary to the Bribery Act 2010
- wilfully or negligently causing harm or injury to another employee, client, customer or visitor, physical violence, assault, fighting, bullying or grossly offensive, abusive or aggressive behaviour or language
- deliberately or negligently causing loss or damage to the Company's property, or to property belonging to another employee, client, customer or visitor
- vandalism of, or otherwise intentionally interfering with, the Company's computers or computer or telephone network
- serious carelessness or gross negligence, including grossly negligent acts or omissions

- dereliction of duty, including sleeping whilst at work and undertaking unauthorised activities during normal working hours
- wilful refusal to obey a reasonable management instruction or serious insubordination
- serious incapacity at work through an excess of alcohol or illegal drugs, whether consumed on or off Company premises but which affects the employee's ability to carry out their job duties whilst at work
- bringing illegal drugs or other illegal substances or items or weapons on to Company premises
- smoking on Company premises, other than in designated outside smoking areas
- logging on to sexually explicit websites, downloading or circulating pornographic or other offensive, illegal or obscene material or using the Internet or e-mail for gambling, illegal activities or the sending of offensive e-mails (e.g. jokes) to work colleagues (in the latter case, including from the employee's home computer in their own time)
- engaging in sexual activity on Company premises at any time
- posting derogatory, offensive, discriminatory or defamatory comments online (for example, on social media websites) about the Company, its employees, clients or customers or otherwise conducting themselves online in a way that is detrimental to the Company or brings the Company into serious disrepute
- a serious breach of health and safety rules, including acts or omissions which endanger the safety of another employee, client, customer or visitor
- a serious breach of security rules
- behaviour outside working hours or work location, which either results in or has the potential to result in criminal charges or convictions, which affect the employee's ability to perform their job duties
- discriminating against, harassing, bullying or victimising another employee, client, customer or visitor because of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race (including colour, nationality and ethnic or national origins), religion or belief, sex and/or sexual orientation
- a serious breach of confidentiality, including unauthorised access of computer and personnel records and communicating or leaking trade secrets or confidential information about the Company or its employees, clients or customers to third parties
- working for a competitor without permission
- engaging in an unauthorised activity which conflicts with the interests of the Company or its clients or customers
- breaching copyright or any other proprietary interest belonging to the Company

- knowingly breaking a legal requirement in connection with employment
- bringing the Company into serious disrepute, even if done in the employee's own time
- unauthorised absence, including failure to return from a period of annual leave or other approved leave of absence.

The above is intended as a guide and is not an exhaustive list.

16 DISCIPLINARY PROCEDURES

Disciplinary Procedure

The purpose of this section is to indicate clearly how alleged problems of discipline will be handled within the Company.

Unless where otherwise stated this Disciplinary Procedure is non-contractual and does not form part of an employee's Contract of Employment.

Where an employee is working with less than twenty four months' continuous service at the date of the commission of any offence or whose performance falls below the standard required, the Company has absolute discretion on whether to apply this procedure in part or whole. Whilst the Company reserves the right to exclude and therefore remove the employee from the procedure in whole, the employee will only be disciplined or dismissed after the appropriate Manager has confirmed the decision to take disciplinary action with one or more of the Directors.

It is an express term of an employee's contract of employment that the Company reserves the right, in appropriate cases, to implement a demotion as an alternative to more serious disciplinary action. If demotion is chosen the rate of pay and other terms that apply will be those that are appropriate to the new position occupied.

Right to be accompanied

When required or invited to attend a formal disciplinary or appeal hearing (i.e. not an informal interview or counselling session) you are entitled by law to make a reasonable request to be accompanied to the hearing by either:

- an employee colleague;
- a full time official employed by a trade union; or
- a lay trade union official so long as they have written certification from their union that they have experience of or have received training in acting as an employee's companion at disciplinary hearings.
- If your chosen companion cannot attend the disciplinary hearing on the date proposed by the Company you may request an alternative date so

long as this is reasonable and falls within five working days beginning with the working day originally suggested. If you are suspended from work on full pay, your suspension may be continued until the hearing takes place. Legal representation will not be recognised.

Your companion has a legal right to address the hearing in order to put or to sum up your case, respond on your behalf to any view expressed at the hearing and to confer with you. Your companion may ask questions of any witness but cannot answer questions on your behalf. Your companion may not address the meeting or ask questions of any witness if you do not wish it.

Breaches of Disciplinary Rules

Gross Misconduct

In the event of an employee allegedly committing an act which is deemed to be Gross Misconduct, a full investigation of the circumstances leading up to the incident will be conducted. In most cases it is more appropriate for the employee to be suspended on full pay during the investigation.

The full investigation in order to establish all the facts of the situation will be conducted. All the evidence so gathered will be presented to the employee concerned.

If, having heard all the evidence, the decision is one of dismissal, the employee has the right of appeal to an alternative person, not involved with the original decision. The employee has the right to be accompanied and represented at the appeal.

Employees dismissed for Gross Misconduct have no right to any period of notice or to receive payment for any outstanding contractual accrued holidays.

Offences other than Gross Misconduct

One of the responsibilities of Supervision is the maintenance of good conduct within the Company on a day to day basis. For this reason it may be necessary to reprimand individual employees for the purpose of emphasising and encouraging improvements in an individual's conduct. Each offence will be handled in accordance with the following procedure, with a record maintained of each stage.

The Company reserves the right to enter the disciplinary procedure at any stage depending on the circumstances and severity of the offence.

Stages of Warning

In cases of Offences other than Gross Misconduct, the following stages of warning will apply:

Verbal warning
If your conduct does not meet acceptable standards you will normally be given a

formal VERBAL WARNING. You will be advised in writing of the reason for the warning and of your right to appeal. A brief note of the verbal warning will be kept but it will be disregarded for disciplinary purposes after 6 months, subject to your satisfactory conduct.

Written warning

If the offence is a serious one and a verbal warning is inappropriate, or if a previous offence is re-committed within 6 months, a WRITTEN WARNING may be given to you. This will give details of the complaint, the improvement required and the timescale. It will warn that a FINAL WRITTEN WARNING may be given if there is no satisfactory improvement within the specified time and will advise you of your right to appeal. A copy of this written warning will be kept on your personnel file but it will be disregarded for disciplinary purposes after 6 months subject to satisfactory conduct.

Final written warning

If there is still a failure to improve and or your conduct is still unsatisfactory, or if the misconduct is sufficiently serious to warrant only one written warning but insufficiently serious to justify dismissal (in effect both first and final written warnings), a FINAL WRITTEN WARNING will normally be given to you. This will give details of the complaint against you, will warn that dismissal may result if there is no satisfactory improvement within a specified time and will advise you of your right to appeal. A copy of this final written warning will be kept on your personnel file but it will be disregarded for disciplinary purposes after 12 months (in exceptional cases the period may be longer) subject to satisfactory conduct.

The warning will state the nature of the offence and the action necessary by the employee to remedy the situation. In addition, it will state clearly that suspension without pay and ultimately dismissal will occur in the event of any future occurrences.

Dismissal

Failure to meet the requirements set out in the final written warning will normally lead to DISMISSAL with appropriate notice. A decision of this kind will only be made after the fullest possible investigation. Dismissal can be authorised only by a senior manager or a Director. The employee will be informed of the reasons for dismissal, the appropriate period of notice, the date on which his or her employment will terminate and how the employee can appeal against the dismissal decision.

In circumstances that would, in the Company's opinion, otherwise justify dismissal the Company may, in its absolute discretion, vary your duties including demoting you as an alternative disciplinary action.

Suspension without Pay

Suspension from the Company without pay for a period not exceeding five working days may be given as a alternative to dismissal, if appropriate. A copy of the letter confirming the suspension without pay will be given to the individual and a copy kept in the individual's personnel file. The letter will also state that ultimately dismissal will occur in the event of any future occurrences.

Disciplinary Appeals

At the end of a disciplinary hearing, you will be informed both verbally and in writing of your right of appeal, including the name of the person to whom your appeal should be made.

If you decide to appeal, you must give written Notice of Appeal to the nominated person. The notice must be received within 5 working days from the day on which you received the written confirmation of the disciplinary hearing decision.

The Notice of Appeal must state whether you are appealing against the conduct of the disciplinary hearing, its finding, the penalties imposed, or a combination of these factors and the supporting reasons for your appeal.

Our aim in providing an appeal system is to ensure that you have the facility for a complete re-appraisal of the facts and procedures and to reconsider the soundness of the earlier decision.

The Appeal Hearing will be conducted by a person who has previously not been involved in the disciplinary process, so that the original disciplinary hearing can be examined to establish whether the hearing was a full and thorough airing and examination of all the facts/evidence, proper procedures were observed, the findings were fair and reasonable and the penalty imposed properly reflected the gravity of the offence and any mitigating factors were fully considered.

The format of an Appeal Hearing, will be an opportunity for you to present your supporting reasons as to why you believe the disciplinary action taken is either unfair, or too harsh. You may submit any appropriate evidence and call any appropriate witness on your behalf.

At an Appeal Hearing you are again entitled to be accompanied by a work colleague of your choice, or a Trade Union representative. Legal representation will not be recognised.

The findings, decision and outcome of the Appeal Hearing, will be confirmed to you in writing.

17 GRIEVANCE PROCEDURE

Introduction

This procedure is entirely non-contractual and **does not** form part of your contract of employment with the Company.

We know that problems and tensions can arise between people at work and that if such issues are not dealt with and resolved quickly, they may well get worse rather than better. Accordingly, we have established our Grievance Procedure, the use of which is open to you at any time. The purpose of the procedure is firstly to allow you freely to express a complaint or matter of concern and then, to try and resolve the issue raised by means of a discussion and agreed solution.

The procedure is not intended to prevent minor, day to day issues being resolved informally by means of bringing the matter to the attention of your Supervisor/Line Manager without written record.

However, should you wish to have a grievance formally investigated and recorded, you must submit your grievance in writing, giving full details of the matter. This should be addressed to your Line Manager, who will then arrange a meeting to discuss the matter.

If the matter is not satisfactorily resolved at this point, you should appeal in writing to the next level of management who shall be the final arbiter in this procedure.

You are entitled to be accompanied at any grievance hearing by a work colleague of your choice, or your Trade Union Representative. Legal representation will not be recognised.

18 GDPR DATA PROTECTION POLICY

Definitions

In this policy, the following words and phrases have the following meanings:

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

"Criminal records personal data" means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.

"Data protection legislation" means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

“Data subject” means a living identified or identifiable individual about whom the Company holds personal data.

“Member of staff” is any director, employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the Company.

“Personal data” is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

“Processing” is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

“Special categories of personal data” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject’s sex life or sexual orientation.

Introduction

This policy sets out how the Company processes the personal data of data subjects, including the personal data of job applicants and the personal data of our current and former directors, employees, workers, agency workers, apprentices, interns, volunteers, contractors, consultants, clients, customers, suppliers and other third parties. It applies to all personal data that we process, regardless of the media on which those personal data are stored, e.g. electronically, on paper or on other materials. The Company is committed to being clear and transparent about how we collect and use personal data and to complying with our data protection obligations. Protecting the confidentiality, security and integrity of the personal data that we process is also of paramount importance to our business operations. The Company will process personal data relating to you in accordance with this policy, the data protection legislation and the latest privacy notice which has been issued to you.

This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

As a member of staff, you are yourself a data subject and you may also process personal data on the Company’s behalf about other data subjects. This policy should

therefore be read and interpreted accordingly. You must always comply with it when processing personal data on the Company's behalf in the proper performance of your job duties and responsibilities. The data protection legislation contains important principles affecting personal data relating to data subjects. The purpose of this policy is to set out what we expect from you and to ensure that you understand and comply with the rules governing the processing of personal data to which you may have access in the course of your work, so as to ensure that neither the Company nor you breach the data protection legislation.

The Company takes compliance with this policy very seriously. Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the Company's disciplinary procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without the Company's consent, constitutes a gross misconduct offence and could lead to your summary dismissal. If you are not an employee, you may have your contract with the Company terminated with immediate effect.

The Company's data protection officer has responsibility for data protection compliance within the business. You should contact them if you have any questions about the operation of this policy or you need further information about the data protection legislation, or if you have any concerns that this policy is not being or has not been followed. They can be contacted as follows: Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA. You must also contact them to seek further advice in the following circumstances:

- if you are in any doubt about what you can or cannot disclose and to whom
- if you are unsure about the lawful basis you are relying on to process personal data
- if you need to rely on consent to process personal data
- if you need to obtain or issue privacy notices
- if you are not clear about the retention period for the personal data being processed
- if you are unsure about what appropriate security measures you need to implement to protect personal data
- if you need assistance in dealing with any rights invoked by a data subject
- if you suspect there has been a personal data breach
- where you propose to use personal data for purposes other than that for which they were collected
- where you intend to engage in a significant new or amended data processing activity
- where you plan to undertake any activities involving automated decision-making, including profiling
- if you need assistance with, or approval of, contracts in relation to sharing personal data with third-party service providers

- if you believe personal data are not being kept or deleted securely or are being accessed without the proper authorisation
- if you suspect there has been any other breach of this policy or any breach of the data protection principles

If you wish to make an internal complaint that this policy is not being or has not been followed, you can also raise this as a formal grievance under the Company's grievance procedure.

The data protection principles

Under the data protection legislation, there are six data protection principles that the Company and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

4. Accurate and, where necessary, kept up to date; every reasonable step must also be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

The Company is responsible for, and must be able to demonstrate compliance with, these data protection principles. This is called the principle of accountability.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

This principle means that both the Company and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

Lawfulness and fairness

The data protection legislation provides that processing is only lawful in certain circumstances. These include where:

- the data subject has given consent to the processing of their personal data for one or more specific purposes
- the processing is necessary for the performance of a contract with the data subject, e.g. an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with our legal obligations
- the processing is necessary to protect the data subject's vital interests (or someone else's vital interests)
- the processing is necessary to pursue our legitimate interests (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override our interests; the purposes for which we process personal data for legitimate interests must also be set out in an appropriate privacy notice

The Company and members of staff must only process personal data on the basis of one or more of these lawful bases for processing. Before a processing activity starts for the first time, and then regularly while it continues, we will review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and satisfy ourselves that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will conduct a legitimate interests assessment, keep a record of it and keep it under review.

Where the Company relies on consent as the lawful basis for processing, this requires the data subject to have given a positive statement, active opt-in or clear affirmative action; pre-ticked boxes, inactivity or silence do not constitute consent. If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so you must ensure that you obtain separate consents for different types of processing, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

The data protection legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional

requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

- the data subject has given their explicit consent to the processing of their personal data for one or more specified purposes; explicit consent requires a very clear and positive statement and it cannot be implied from the data subject's actions
- the processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the Company or the data subject under employment law or social security law
- in the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the data subject
- the processing is necessary for the establishment, exercise or defence of legal claims
- (*insert any other applicable lawful basis for processing special categories of personal data, as set out in the GDPR).*

We may from time to time need to process special categories of personal data and criminal records personal data. The Company and members of staff must only process special categories of personal data and criminal records personal data where there is also one or more of these special lawful bases for processing. Before processing any special categories of personal data and criminal records personal data, you must notify our data protection officer so that they may assess whether the processing complies with one or more of these special conditions.

A clear record must be kept of all consents, including explicit consents, which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables the Company to demonstrate compliance with the data protection requirements for consent.

Transparency

Under the data protection legislation, the transparency principle requires the Company to provide specific information to data subjects through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices may comprise general privacy statements applicable to a specific group of data subjects, e.g. employees, or they may be stand-alone privacy statements covering processing related to a specific purpose. Whenever we collect personal data directly from data subjects, including for employment purposes, we must provide the data subject with all the information required to be included in a privacy notice. This includes:

- the identity and contact details of the Company (as data controller) and any representative
- where applicable, the identity and contact details of the data protection officer

- the purposes for which the personal data will be processed
- the lawful basis or bases for processing
- where we are relying on our legitimate interests (or those of a third party) as the lawful basis for processing, what those legitimate interests are
- the categories of personal data, unless they were obtained directly from the data subject
- the third-party sources that the personal data originate from, unless they were obtained directly from the data subject
- the recipients, or categories of recipients, with whom the personal data may be shared
- details of transfers to non-EEA countries and the suitable safeguards applied
- the retention period for the personal data or, if that is not possible, the criteria to be used to determine the retention period
- the existence of the data subject's rights, i.e. subject access, rectification, erasure, restriction of processing, objection and data portability
- the right to withdraw consent to processing at any time, where consent is being relied on as the lawful basis for processing
- the right to lodge a complaint with the Information Commissioner's Office
- whether the provision of personal data is part of a statutory or contractual requirement or obligation, or a requirement necessary to enter into a contract, and the possible consequences of failing to provide the personal data
- the existence of any automated decision-making, including profiling, and meaningful information about how decisions are made, the significance and consequences.

We must issue a privacy notice, which can be by electronic means, when we first collect a data subject's personal data from them. If the personal data have been obtained from third parties, we must provide the privacy notice information within a reasonable period of having obtained the personal data, but at the latest within one month. However, if the personal data are to be used to communicate with the data subject, the privacy notice information is to be provided, at the latest, when the first communication takes place, or if disclosure of the personal data to another recipient is envisaged, it is to be provided, at the latest, when the data are first disclosed. You must comply with these rules on privacy notices when processing personal data on the Company's behalf in the proper performance of your job duties and responsibilities.

The Company will issue privacy notices to you from time to time.

Privacy notices can also be obtained from the Company's data protection officer.

Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, for example in an appropriate privacy notice, unless the data subject has been informed of the new purposes and the terms of this policy are otherwise complied with, e.g. there is a lawful basis for processing. This also includes special categories of personal data and criminal records personal data.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will only collect personal data to the extent that they are required for the specific purposes notified to the data subject. You must only process personal data where your job duties and responsibilities require it and you must not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, you must ensure that any personal data you collect are adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with the Company's rules on data retention and destruction set out below.

Accuracy

Personal date must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

It is important that the personal data we hold about you as a data subject is accurate and up to date. Please keep us informed if your personal data changes, e.g. you change your home address, so that our records can be updated. The Company cannot be held responsible for any errors in your personal data in this regard unless you have notified the Company of the relevant change. We will promptly update your personal data if you advise us that they have changed or are inaccurate.

You must also ensure that the personal data we hold about other data subjects is accurate and up to date where this is part of your job duties or responsibilities. This includes special categories of personal data and criminal records personal data. You must check the accuracy of any personal data at the point of their collection and at regular intervals thereafter. You must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

Storage limitation

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

The Company will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special categories of personal data and criminal records personal data. You must comply with the Company's rules on data retention and destruction set out below.

Retention: job applicants

If a job applicant's application for employment or engagement is unsuccessful, the Company will generally hold their personal data, including special categories of personal data and criminal records personal data, for [six months] [one year] after the end of the relevant recruitment exercise but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to [six years] to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court.

If the job applicant has consented to the Company keeping their personal data on file for in case there are future suitable employment opportunities with us, we will hold their personal data for a further one year after the end of the relevant recruitment exercise, or until they withdraw their consent if earlier.

Retention: members of staff

The Company will generally hold personal data, including special categories of personal data and criminal records personal data, for the duration of a member of staff's employment or engagement. The exceptions are:

- any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship
- criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by the Company as relevant to the ongoing working relationship
- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the Company as relevant to the ongoing working relationship
- if it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after [six months] or once the

conviction is “spent” if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession)
- disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment).

Once a member of staff has left employment or their engagement has been terminated, we will generally hold their personal data, including special categories of personal data and criminal records personal data, for [one year] after the termination of their employment or engagement, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to [six years] to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. We will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to [six years] after the termination of their employment or engagement.

Overall, this means that we will “thin” the file of personal data that we hold on members of staff [one year] after the termination of their employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Retention: other third parties, including clients, customers and suppliers

The Company will generally hold personal data, including special categories of personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of our business relationship with them.

Once our business relationship with a client, customer or supplier has been terminated, we will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of the business relationship, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to [six years] to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a County Court or High Court.

Overall, this means that we will “thin” the file of personal data that we hold on clients, customers and suppliers [one year] after the termination of the business relationship, so that we only continue to retain for a longer period what is strictly necessary.

Destruction and erasure

All personal data, including special categories of personal data and criminal records personal data, must be reviewed before destruction or erasure to determine whether

there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above. If you are responsible for maintaining personal data and are not clear what retention period should apply to a particular record, please contact our data protection officer for guidance.

Personal data which are no longer to be retained will be permanently erased from our IT systems or securely and effectively destroyed, e.g. by cross-shredding of hard copy documents, burning them or placing them in confidential waste bins or by physical destruction of storage media, and we will also require third parties to destroy or erase such personal data where applicable. You must take all reasonable steps to destroy or erase personal data that we no longer require.

In some circumstances we may anonymise personal data so that they no longer permit a data subject's identification. In this case, we may retain such personal data for a longer period.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Company takes the security of personal data seriously and we have implemented and maintain safeguards which are appropriate to the size and scope of our business, the amount of personal data that we hold and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. We have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. We regularly test and evaluate the effectiveness of our technical and organisational safeguards to ensure the security of our processing activities.

In turn, you are responsible for protecting the personal data that we hold, and you must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage. You must be particularly careful in protecting special categories of personal data and criminal records personal data. You must follow all procedures, and comply with all technologies and safeguards, that we put in place to maintain the security of personal data from the point of collection to the point of destruction.

Where the Company uses third-party service providers to process personal data on our behalf, additional security arrangements need to be implemented in contracts with those third parties to safeguard the security of personal data. You can only share personal

data with third-party service providers if you have been authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services
- sharing the personal data complies with the privacy notice that has been provided to the data subject (and, if required, the data subject's consent has been obtained)
- the third party has agreed to comply with our data security procedures and has put adequate measures in place in ensure the security of processing
- the third party only acts on our documented written instructions
- a written contract is in place between the Company and the third party that contains specific approved terms
- the third party will assist the Company in allowing data subjects to exercise their rights in relation to data protection and in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments
- the third party will delete or return all personal data to the Company at the end of the contract
- the third party will submit to audits.

Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, you must seek the approval of its terms from our data protection officer.

You may only share personal data with other members of staff if they have a business need to know in order to properly perform their job duties and responsibilities.

Hard copy personnel files, which hold personal data gathered during the working relationship, are confidential and must be stored in locked filing cabinets. Only authorised members of staff, who have a business need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.

The Company has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

The data protection legislation requires the Company to notify any personal data breach

to the Information Commissioner's Office within 72 hours after becoming aware of the breach and, where there is a high risk to the rights and freedoms of data subjects, to the data subject themselves. A personal data breach is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises the confidentiality, integrity or availability of personal data or the safeguards that we, or our third-party service providers, have put in place to protect them. The Company has procedures in place to deal with any suspected personal data breach and you are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact our data protection officer, retain any evidence you have in relation to the breach and follow the Company's data breach policy and response plan.

Accountability

The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles. This means that we must implement appropriate and effective technical and organisational measures to ensure compliance and we also require you to fully assist and co-operate with us in this regard. In particular, we have:

- appointed a data protection officer to be responsible for data protection compliance and privacy matters within the business
- kept written records of personal data processing activities
- implemented a privacy by design approach when processing personal data and we will conduct and complete data protection impact assessments (DPIAs) where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system, in particular using a new technology, is likely to result in a high risk to the rights and freedoms of data subjects
- integrated data protection requirements into our internal documents, including this data protection policy, other related policies and privacy notices
- introduced a regular training programme for all members of staff on the data protection legislation and on their data protection duties and responsibilities and we also maintain a training record to monitor its delivery and completion – you must undergo all mandatory data protection training
- introduced regular reviews of our privacy measures and our policies, procedures and contracts and regular testing of our systems and processes to monitor and assess our ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

We also keep records of our personal data processing activities and you are required to assist us in ensuring these records are full, accurate and kept up to date.

Privacy by design and data protection impact assessments

We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation. You must assess what privacy by design measures can be implemented on all processes or systems that process personal data where this is part of your job duties or responsibilities because those processes or systems are under your control.

Where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system which is under your control, is likely to result in a high risk to the rights and freedoms of data subjects, you must assist us in conducting and completing a DPIA. This includes (but is not limited to):

- systematic and extensive automated processing and automated decision-making activities, including profiling, and on which decisions are based that have legal effects, or similar significant effects, on data subjects
- large-scale processing of special categories of personal data or criminal records personal data
- large-scale systematic monitoring of publicly accessible areas, e.g. using CCTV.

Before any form of new technology, program, process or system is introduced, you must contact our data protection officer in order that a DPIA can be carried out.

A DPIA will comprise a review of the new technology, program, process or system and it must contain a description of the processing operations and the purposes, an assessment of the necessity and proportionality of the processing in relation to those purposes, an assessment of the risks to individuals and the measures in place to address or mitigate those risks and demonstrate compliance.

Automated processing and automated decision-making

Automated processing is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, and automated decision-making occurs when an electronic system uses an individual's personal data to make a decision without human intervention.

The Company does not carry out any automated processing and does not take any decisions based solely on automated decision-making, including profiling.

Direct marketing

The Company is subject to certain rules when marketing our clients and customers. If you are involved in direct marketing to customers, you must comply with the Company's guidelines on this. In particular, a data subject's prior consent is required for electronic direct marketing. There is a limited exception for existing clients and customers which allows us to send marketing texts and e-mails if we have obtained their contact details in

the course of a sale to that person, we are marketing similar products or services to them and we gave that person an opportunity to opt out of marketing when first collecting their details and in every subsequent message.

If a data subject objects to direct marketing, it is essential that this is actioned in a timely manner and their details should be suppressed as soon as possible. You can retain just enough information to ensure that marketing preferences are respected in the future.

Transferring personal data outside the European Economic Area

The data protection legislation restricts transfers of personal data to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to data subjects is maintained.

The Company does not transfer personal data to countries outside the EEA and you must ensure that you comply with this rule.

Data subject rights to access personal data

Under the data protection legislation, data subjects have the right, on request, to obtain a copy of the personal data that the Company holds about them by making a written data subject access request (DSAR). This allows the data subject to check that we are lawfully processing their personal data. The data subject has the right to obtain:

- confirmation as to whether or not their personal data are being processed
- access to copies of their specified personal data
- other additional information.

The other additional information (which should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language) comprises:

- the purposes of the processing and the categories of personal data concerned
- the recipients, or categories of recipients, to whom the personal data have been or will be disclosed, in particular recipients in non-EEA countries
- where the personal data are transferred to a non-EEA country, what appropriate safeguards are in place relating to the transfer
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the data subject's rights to request rectification or erasure of their personal data or restriction of processing of their personal data or to object to such processing
- their right to lodge a complaint with the Information Commissioner's Office if they think the Company has failed to comply with their data protection rights
- where the personal data are not collected from them, any available information as to their source

- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the envisaged consequences of such processing for them.

When a data subject makes a DSAR, we will log the date on which the request was received and confirm their identity. Where we have reasonable doubts concerning the data subject's identity, we will request them to provide such additional information necessary to confirm their identity before complying with their DSAR. We will then search databases, systems and other places where the personal data which are the subject of the DSAR may be held. Where we process a large quantity of personal data about a data subject, we may ask them to first specify the information that their DSAR relates to.

If the data subject makes their DSAR electronically, the Company must provide a copy of the personal data in a commonly used electronic format, unless they specifically request otherwise. If the data subject wants additional copies of the personal data, the Company will charge a reasonable fee, which is based on our administrative costs of providing the additional copies.

The Company will normally respond to a DSAR and provide copies of the personal data within one month of the date of receipt of the request. However, we may extend this time limit for responding by a further two months if the request is complex or there are a number of requests made by the data subject. If we intend to extend the time limit, we will contact the data subject within one month of the DSAR's receipt to inform them of the extension and to explain why it is necessary.

Before providing the personal data to the data subject making the DSAR, we will review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data. We will also check whether there are any statutory exemptions from disclosure that apply to the personal data that are the subject of the DSAR. If a statutory exemption applies to any of the personal data, those personal data may not be disclosed.

Whilst we will normally provide a copy of the personal data in response to a DSAR free of charge, we reserve the right to charge a reasonable fee, based on our administrative costs of providing the personal data, when a DSAR is manifestly unfounded or excessive, particularly if it repeats a DSAR to which we have already responded. Alternatively, where a DSAR is manifestly unfounded or excessive, we reserve the right to refuse to respond altogether. Where we refuse to act on a request in this way, we will set out our written reasons why to the data subject within one month of receipt of their DSAR. We will also inform them of their right to complain to the Information Commissioner's Office or to seek a judicial remedy in the courts.

If you wish to exercise your data subject access rights, please complete our data subject access request form, or put the request in an e-mail, and send it to our data protection officer as follows: Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA. We will inform you if we need to further verify your identity.

If you receive a DSAR from another data subject, you must immediately forward it to our data protection officer and they will deal with responding to it.

Other data subject rights in relation to their personal data

Data subjects have a number of other rights in relation to their personal data. When we process data subjects' personal data, we will respect those rights. It is the Company's policy to ensure that requests by data subjects to exercise their rights in respect of their personal data are handled in accordance with the data protection legislation.

Subject to certain conditions, and in certain circumstances, data subjects have the right to:

- be informed – this is normally satisfied by issuing them with an appropriate privacy notice
- request rectification of their personal data - this enables them to have any inaccurate or incomplete personal data we hold about them corrected or completed, including by their providing a supplementary statement
- request the erasure of their personal data - this enables them to ask us to delete or remove their personal data where there's no compelling reason for their continued processing, e.g. it's no longer necessary in relation to the purpose for which they were originally collected or if there are no overriding legitimate grounds for the processing
- restrict the processing of their personal data - this enables them to ask us to suspend the processing of their personal data, e.g. if they contest the accuracy and so want us to verify the accuracy or the processing is unlawful but they don't want the personal data to be erased
- object to the processing of their personal data - this enables them to ask us to stop processing their personal data where we are relying on the legitimate interests of the business as our lawful basis for processing and there is something relating to their particular situation which makes them decide to object to processing on this ground
- data portability - this gives them the right to request the transfer of their personal data to another party so that they can reuse them across different services for their own purposes
- not be subject to automated decision-making, including profiling - this gives them the right not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them

- prevent direct marketing - this enables them to prevent our use of their personal data for direct marketing purposes
- be notified of a data breach which is likely to result in a high risk to their rights and freedoms.

If, as a data subject, you wish to exercise any of these rights, please contact our data protection officer.

If a data subject invokes any of these rights, you must take steps to verify their identity, log the date on which the request was received and seek advice from our data protection officer if you need assistance in dealing with the matter. The following response procedures apply as applicable:

- response to requests to rectify personal data - unless there is an applicable exemption, we will rectify the personal data without undue delay and we will also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed, e.g. our third-party service providers, unless this is impossible or involves disproportionate effort
- response to requests for the erasure of personal data - we will erase the personal data without undue delay provided one of the grounds set out in the data protection legislation applies and there is no applicable exemption (and, where the personal data are to be erased, a similar timetable and procedure to that applying to responding to DSARs will be followed). We will also communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. Where we have made the personal data public, we will take reasonable steps to inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data
- response to requests to restrict the processing of personal data - where processing has been restricted in accordance with the grounds set out in the data protection legislation, we will only process the personal data (excluding storing them) with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. Prior to lifting the restriction, we will inform the data subject that it is to be lifted. We will also communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort
- response to objections to the processing of personal data - where such an objection is made in accordance with the data protection legislation and there is no applicable exemption, we will no longer process the data subject's personal data unless we can show compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or we are processing the personal data for the establishment, exercise or defence of legal claims. If a data subject objects to the processing of their personal data for direct marketing purposes, we will stop

processing the personal data for such purposes

- response to requests for data portability - unless there is an applicable exemption, we will provide the personal data without undue delay if the lawful basis for the processing of the personal data is consent or pursuant to a contract and our processing of those data is carried out by automated means (and a similar timetable and procedure to that applying to responding to DSARs will be followed)

In the limited circumstances where the data subject has provided their consent to the processing of their personal data for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on consent before its withdrawal.

If, as a data subject, you wish to withdraw your consent to the processing of your personal data for a specific purpose, please contact our data protection officer. Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purpose you originally agreed to, unless we have another lawful basis for processing.

If a data subject invokes their right to withdraw their consent, seek advice from our data protection officer if you need assistance in dealing with the matter.

Data subjects also have the right to make a complaint to the Information Commissioner's Office at any time.

Your obligations in relation to personal data

You must comply with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of the Company in the proper performance of your job duties and responsibilities. We rely on you to help us meet our data protection obligations to data subjects.

Under the data protection legislation, you should also be aware that you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence for you knowingly or recklessly to obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of the Company. This would include, for example, taking clients' or customers' contact details or other personal data without the Company's consent on the termination of your employment, accessing another employee's personal data without authority or otherwise misusing or stealing personal data held by the Company. It is also a criminal offence to knowingly or recklessly re-identify personal data that has been anonymised without the consent of the Company, where we de-identified the personal data, and it is a criminal offence to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a data subject following a data subject access request. Where unlawful activity is suspected, the Company will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the data protection legislation and this may

result in criminal proceedings being instigated against you. The Company may also need to report the alleged breach to a regulatory body. This conduct would also amount to a gross misconduct offence under the Company's disciplinary procedure and could lead to your summary dismissal.

You must also comply with the following guidelines at all times:

- only access personal data that you have authority to access and only for authorised purposes, e.g. if you need them for the work you do for the Company, and then only use the data for the specified lawful purpose for which they were obtained
- only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form. unless the data subject has given their explicit consent to this
- be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request
- where the Company provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Company's requirements in this regard
- only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail
- if you receive a request for personal data about another member of staff or data subject, you should forward this to the Company's data protection officer
- ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with Company rules on computer access and secure file storage
- do not access another member of staff's personal data, e.g. their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence
- do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without the Company's consent as this will be treated as gross misconduct and it is a criminal offence
- do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by

your line manager

- ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- do not store personal data on local computer drives, your own personal computer or on other personal devices
- do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by cross-shredding hard copies
- ensure that you attend all mandatory data protection training
- refer any questions that you may have about the data protection legislation or compliance with this policy to our data protection officer
- remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

Changes to this policy

The Company will review this policy at regular intervals and we reserve the right to update or amend it at any time and from time to time. We will circulate any modified policy to members of staff and, where appropriate, we may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, the Company will comply with the data protection legislation.

This policy may also be made available to the Information Commissioner's Office on request.

19 USE OF COMPANY COMPUTER POLICY

Computer usage

Some employees have access to computers at work for use in connection with the Company's business. Computers are provided to employees to undertake business-related activities only. Employees who are discovered unreasonably using the Company's computers for personal and private purposes will be dealt with under the Company's disciplinary procedure.

Vandalism of, or otherwise intentionally interfering with, the Company's computers, systems or networks constitutes a gross misconduct offence and could render the employee liable to summary dismissal.

Security

You are responsible for the security of the computer equipment allocated to or used by you, and you must not allow it to be used by anyone else other than in accordance with this policy.

As many computer files contain some form of confidential or otherwise sensitive business information or personal data, the Company takes the security of these files very seriously. With this in mind, we have introduced some security precautions that all employees must abide by.

These are as follows:

- if you need to leave your computer for more than a couple of minutes, lock the computer screen
- if you need to leave your computer for a long period of time, log off - never leave an unattended computer logged on
- do not move or tamper with desktop computers and cabling for computer equipment without first consulting the IT department
- use passwords on all computer equipment
- computer passwords are considered our confidential information even if you are using your personal password for social networking to login to our work systems. When creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member - passwords should preferably be a mix of upper and lower case letters, special characters and numbers and should not be the same as any other personal passwords you may have (such as Internet banking passwords)
- always keep your password private, do not write it down and do not divulge it to anyone else (including other members of staff), except for a Director
- if you suspect that someone knows your password, change it in the normal way
- change your password at regular intervals in any event
- never use anyone else's username and password and do not allow anyone else to log on using your username and password, unless authorised by a Director
- always shut down your computer when you go home at the end of the day
- if you notice any suspicious activity, for example an employee trying to gain unauthorised access to another member of staff's computer, notify your manager immediately
- if you have been issued with a Company laptop computer, tablet computer, smartphone or other mobile device, keep it secure at all times, particularly

when travelling. Passwords and encryption must be used to secure access to data kept on such equipment to ensure that confidential or other sensitive business information or personal data is protected in the event of loss or theft and you must take such other precautions as we may require from time to time against compromising security

- if you are provided with a Company computer for use in your home, family members are not allowed to use it
- always comply with the terms of the Company's data protection policy in relation to ensuring the security of personal data held on computer, in particular the sections in that policy on integrity and confidentiality and your obligations in relation to personal data
- do not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties

Data

The computers and the data they contain (including data backed up to cloud-based storage applications) are provided to undertake business-related activities and to enable you to carry out your job duties. As such, you must not delete, amend, destroy, copy or modify existing systems, programs, information or data, unless this is both specifically related to the work you are undertaking and you have the authority to make such deletion, amendment, copy or modification. In particular, you should not delete or amend any documentation or programs which are stored on the Company's network or communal drives (including documentation or programs which are backed up to cloud-based storage applications) unless you have the requisite level of authority to do so.

Non-work related data should not be copied onto or stored on Company computers or on the Company's network or communal drives (including in cloud-based storage applications).

Use of portable storage devices

You must not attach any device or equipment to the Company's computer systems without authorisation from the IT department. This includes portable storage devices, such as memory sticks, USB flash drives and portable hard drives, plus smartphones, tablets and similar devices, whether connected via the USB port or in any other way.

Any employee who transfers files to a third party without permission is likely to be subject to disciplinary action. In the event that this involves the deliberate transfer of sensitive commercial information to a competitor or a serious breach of data protection provisions, it will be treated as gross misconduct.

Software

The Company licences the use of computer software from a variety of outside companies. The Company does not own this software and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Contravention is a disciplinary matter and will be dealt with in accordance with the Company's disciplinary procedure.

Software that you need to use to carry out your job duties will be provided and installed on your computer for you. Installation of any non-approved software from external sources is prohibited. This includes instant messaging programs, photos, video clips, music files, screen savers and wallpapers. Only the IT department has the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses.

Viruses

The Company's computer network makes it vulnerable to viruses. All Company computers have virus protection software installed. Re-configuring or disabling this software is prohibited.

If your computer starts to behave strangely or you suspect it may have become infected with a virus, turn it off immediately and contact the IT department.

Games

Employees may only access any computer games that are on the network outside their normal working hours. You must not install your own games onto your computer.

Remote access

Some employees may spend at least part of their working week on Company business away from the premises. These employees and any others who may work remotely on an informal basis should be aware that all aspects of this policy apply equally to them. Remote working employees will also be expected to comply with any additional guidelines that may be introduced in order to reduce the likelihood of the Company's computer networks or cloud-based storage applications being compromised as a result of remote access.

Employees must not allow any family members or other third parties to either use the Company's computer equipment (including software) or to access or view its internal IT systems or networks.

Temporary workers

From time to time, the Company may need to use temporary staff in order to cover busy periods or annual leave. Should any temporary worker need to use a computer as part of their job role, the manager responsible for their day-to-day supervision will be required to bring this policy and its contents to their attention.

It is also Company policy that any temporary workers who are required to use a computer for more than 14 days will be given their own log-in details. Managers will need to identify if there are any directories or computer files on the computer that will be used by the temporary worker that are of a sensitive or confidential nature. If so, the IT department will need to be involved in restricting access to them. The same principles apply to any self-employed contractors engaged by the Company.

Managers' duties

Managers will be required to notify the IT department in advance of any computer users that will be leaving the Company. This should be done at least seven days before the employee leaves, so that the individual's account can be closed down on their departure.

Likewise, managers should notify the IT department in advance of any new computer users that will be starting work for the Company. This should be done at least seven days before the employee starts, so that the individual's account can be set up ready for their start date.

From time to time, the Company will review its storage of confidential information and the media upon which it is stored (including the use of cloud-based storage applications). Managers will be expected to co-operate in terms of identifying such files, the employees or other staff with access to them and the file locations.

Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company's disciplinary procedure, up to and including summary dismissal for gross misconduct.

20 SOCIAL MEDIA POLICY

Social media definition

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and

business networking websites such as Facebook, MySpace, Bebo, Twitter and LinkedIn. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal blogs. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive. This policy applies in relation to any social media that employees may use.

Use of social media at work

Employees are not permitted to access social media websites or to keep a blog using the Company's IT systems and equipment at any time. This includes laptop and hand-held computers or devices distributed by the Company for work purposes. The Company has added most of the websites of this type to its list of restricted websites. Where employees have their own computers or devices, such as laptops and hand-held devices, they must limit their use of social media on this equipment to outside their normal working hours (for example, during lunch breaks).

However, employees may be asked to contribute to the Company's own social media activities during normal working hours, for example by writing Company blogs or newsfeeds, managing a Facebook account or running an official Twitter or LinkedIn account for the Company. Employees must be aware at all times that, while contributing to the Company's social media activities, they are representing the Company.

Company's social media activities

Where employees are authorised to contribute to the Company's own social media activities as part of their work, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- use the same safeguards as they would with any other type of communication about the Company that is in the public domain
- ensure that any communication has a purpose and a benefit for the Company
- obtain permission from their line manager before embarking on a public campaign using social media
- request their line manager to check and approve content before it is published online
- follow any additional guidelines given by the Company from time to time.

The social media rules set out below also apply as appropriate.

Social media rules

The Company recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Company in these circumstances, employees must be aware that they can still cause damage to the Company if they are recognised online as being one of its employees. Therefore, it is important that the Company has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-Company computers outside the workplace and outside normal working hours, employees must not:

- other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, publicly identify themselves as working for the Company, make reference to the Company or provide information from which others can ascertain the name of the Company
- other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, write about their work for the Company - and, in postings that could be linked to the Company, they must also ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the Company
- conduct themselves in a way that is potentially detrimental to the Company or brings the Company or its clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content
- other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to the Company's website
- allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Company, for example by criticising or arguing with such persons
- include personal information or data about the Company's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs

as long as the Company reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence

- make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees, clients, customers, contractors or suppliers (an employee may still be liable even if the Company, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable)
- make any comments about the Company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation
- disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Company, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of the Company's competitors, for example information about the Company's work, its products and services, technical developments, deals that it is doing or future business plans and staff morale
- breach copyright or any other proprietary interest belonging to the Company, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work - if employees wish to post images, photographs or videos of their work colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by the Company.

Work and business contacts made during the course of employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to the Company and accordingly must be surrendered on termination of employment.

Employees should remember that social media websites are public fora, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their postings on any website will remain private.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for

example by placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees notice any inaccurate information about the Company online, they should report this to their line manager in the first instance.

Social media monitoring

The Company reserves the right to monitor employees' use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- promote productivity and efficiency
- ensure the security of the system and its effective operation
- make sure there is no unauthorised use of the Company's time
- ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- make sure there is no breach of confidentiality.

The Company reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

21 CCTV POLICY

Introduction

The Company uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises, such as clients, customers, contractors and suppliers, and to protect the Company's property. This policy sets out the use and management of the

CCTV equipment and images in compliance with the General Data Protection Regulation, the Data Protection Act 2018 and the Information Commissioner's Office Code of Practice for Surveillance Cameras and Personal Information.

The Company's CCTV facility records images only. There is no audio recording and therefore conversations are not recorded on CCTV (but see the section on covert recording below).

Purposes of CCTV

The purposes of the Company installing and using CCTV systems include to:

- assist in the prevention or detection of crime or equivalent malpractice
- assist in the identification and prosecution of offenders
- monitor the security of the Company's business premises
- ensure that health and safety rules and other Company rules, policies and procedures are being complied with
- assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary or performance management proceedings being instituted against employees and to help in providing relevant evidence
- establish the existence of facts
- promote productivity and efficiency.

The Company is committed to being transparent about how and why CCTV systems are used.

Location of cameras

Cameras are located at strategic points throughout the Company's business premises, principally at the entrance and exit points. The Company has positioned the cameras so that they only cover communal or public areas on the Company's business premises and they have been sited so that they provide clear images. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices. All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate signs are prominently and clearly displayed so that employees, clients, customers and other visitors are aware they are entering an area covered by CCTV.

Recording and retention of images

Images produced by the CCTV equipment are as clear as possible so that they are effective for the purposes for which they are intended. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, are not held for more than one month. Once a hard drive has reached the end of its use, it will be erased prior to disposal. Images that are stored on, or transferred on to, removable media such as CDs are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- the police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness
- prosecution agencies, such as the Crown Prosecution Service
- relevant legal representatives
- line managers involved with Company disciplinary processes
- individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or

prosecution of offenders).

The Managing Director (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of information to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

Individuals' access rights

Under the General Data Protection Regulation, individuals have the right on request to receive a copy of the personal data that the Company holds about them by making a data subject access request, including CCTV images if they are recognisable from the image.

If you wish to exercise your data subject access rights and access any of your CCTV images, please complete our data subject access request form, or put the request in an e-mail, and send it to the Company's data protection officer as follows: Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundells Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA Your request should include the date and time when the images were recorded and the location of the particular CCTV camera, so that the images can be located and your identity can be established as the person in the images. We will inform you if we need to further verify your identity. **Note.** The Company will always check the identity of the employee making the request before processing it.

The data protection officer will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

Covert recording

The Company will only undertake covert recording with the written authorisation of the Managing Director (or another senior director acting in their absence) where there is good cause to suspect that criminal activity or equivalent malpractice is taking, or is about to take, place and informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection. Covert monitoring may include both video and audio

recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will immediately cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the Company cannot reasonably be expected to ignore.

Staff training

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the General Data Protection Regulation and the Data Protection Act 2018 with regard to that system.

Implementation

Stephen McKie is responsible for the implementation of and compliance with this policy and the operation of the CCTV system and they will conduct an annual review of the Company's use of CCTV. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to them.

22 DATA PROTECTION POLICY FOR EMPLOYEES, WORKERS AND CONSULTANTS

Overview

The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy. With immediate effect this policy replaces any previous Data Protection Policy.

The Company collects and processes personal information, or personal data, relating to its employees, workers and contractors to manage the working relationship. This personal information may be held by the Company on paper or in electronic format. Any Data Protection 'consent clause' in it's employees,

workers and contractors contract, or agreement is immediately revoked. The Company has separate policies in place in respect of job applicants and other categories of data subject.

This policy applies to all current and former employees, workers and contractors. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

Data Protection Principles

Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- details of your skills, qualifications, experience and work history, both with previous employers and with the Company;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- photographs;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- any termination of employment or engagement documentation, including resignation letters, dismissal letters, redundancy letters, minutes of meetings, settlement agreements and related correspondence;
- information relating to your performance and behaviour at work including appraisals;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;

- your images (whether captured on CCTV, by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data

'**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement). This includes (see section 'Special Categories' below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;

- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- and
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above bullet point) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Stephen Mckie.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We may also process these special categories of personal information, and information about any criminal convictions and offences, where we have your explicit written consent. In this case, we will first provide you with full details of the personal information we would like and the reason we need it, so that you can properly consider whether you wish to consent or not. It is entirely your choice whether to consent. Your consent can be withdrawn at any time.

The purposes for which we are processing, or will process, these special categories of your personal information, and information about any criminal convictions and offences, are to:

- assess your suitability for employment, engagement or promotion
- comply with statutory and/or regulatory requirements and obligations, e.g. carrying out criminal record checks
- comply with the duty to make reasonable adjustments for disabled employees and workers and with other disability discrimination obligations
- administer the contract we have entered into with you
- ensure compliance with your statutory and contractual rights
- operate and maintain a record of sickness absence procedures
- ascertain your fitness to work
- manage, plan and organise work
- enable effective workforce management
- ensure payment of SSP or contractual sick pay
- meet our obligations under health and safety laws
- make decisions about continued employment or engagement
- operate and maintain a record of dismissal procedures
- ensure effective HR, personnel management and business administration
- ensure adherence to Company rules, policies and procedures
- monitor equal opportunities).

<u>Special Categories</u>
We might process special categories of your personal data for the purposes stated in paragraph '*examples of when we might process your personal data'* which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

Your personal information may be shared internally within the Company, including with members of the HR department, payroll staff, your line manager, other managers in the department in which you work and IT staff if access to your personal information is necessary for the performance of their roles.

The Company may also share your personal information with third-party service providers (and their designated agents), including:

- external organisations for the purposes of conducting pre-employment reference and employment background checks
- payroll providers
- benefits providers and benefits administration, including insurers
- pension scheme provider and pension administration
- occupational health providers
- external IT services
- external auditors
- professional advisers, such as lawyers and accountants

The Company may also share your personal information with other third parties in the context of a potential sale or restructuring of some or all of its business. In those circumstances, your personal information will be subject to confidentiality undertakings.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

We may share your personal information with third parties where it is necessary to administer the contract we have entered into with you, where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of a third party).

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

The Company's Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundells Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.

Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to the Directors on how to do this.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How does the Company protect your personal information?

The Company has put in place measures to protect the security of your personal information. It has internal policies, procedures and controls in place to try and prevent your personal information from being accidentally lost or destroyed, altered, disclosed or used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, workers, agents, contractors and other third parties who have a business need to know in order to perform their job duties and responsibilities. You can obtain further information about these measures from our Data Protection Officer.

Where your personal information is shared with third-party service providers, we require all third parties to take appropriate technical and organisational security measures to protect your personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law. We only allow them to process your personal information for specified purposes and in accordance with our written instructions and we do not allow them to use your personal information for their own purposes.

For how long does the Company keep your personal information?

The Company will only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements.

The Company will generally hold your personal information for the duration of your employment or engagement. The exceptions are:

- any personal information supplied as part of the recruitment process will not be retained if it has no bearing on the ongoing working relationship
- personal information about criminal convictions and offences collected in the course of the recruitment process will be deleted once it has been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by the Company as relevant to the ongoing working relationship
- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the Company as relevant to the ongoing working relationship
- if it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after [six months] or once the conviction is "spent" if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession)
- disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of your employment).

Once you have left employment or your engagement has been terminated, we will generally hold your personal information for one year after the termination of your employment or engagement, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal information for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. We will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for six years after the termination of your employment or engagement. Overall, this means that we will "thin" the file of personal information that we hold on you [one year] after the termination of your employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IT systems and we will also require third parties to destroy or erase such personal information where applicable.

In some circumstances we may anonymise your personal information so that it no

longer permits your identification. In this case, we may retain such information for a longer period.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA. immediately and keep any evidence you have in relation to the breach.

Subject access requests

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

2 Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a subject access request (see above).

You can correct any inaccuracies in your personal data. To do you should contact Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151

426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA.

You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA..

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Data Protection Officer Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's

Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Changes to this policy

The Company reserves the right to update or amend this policy at any time, including where the Company intends to further process your personal information for a purpose other than that for which the personal information was collected or where we intend to process new types of personal information. We will issue you with a new policy when we make significant updates or amendments. We may also notify you about the processing of your personal information in other ways.

Contact

If you have any questions about this policy or how we handle your personal information, please contact our Data Protection Officer as follows: Steven McKie email office@blundellshill.co.uk tel 0151 426 9040 Postal Address Blundell's Hill Golf Club Blundells Lane, Rainhill, Liverpool L35 6NA.

23 ALCOHOL & DRUG POLICY

Policy

Alcohol and or drug consumption can have a detrimental effect on an individual's ability to perform their normal daily duties and may also affect other persons.

In order to promote the general well-being of all its employees and to provide a safe, healthy and congenial working environment, Blundells Hill Golf Club Limited has an Alcohol and Drug Policy.

The aim of this policy is to provide a set of written, agreed procedures and statements to help all employed in the Company to play their part in dealing with employees whose performance and / or behaviour is seriously affected by their misuse of alcohol and drug related problems.

This policy is not intended to apply solely to the so-called alcoholic / addict. The definition of problem drinking / drug taking at work is:

ANY drinking / drug taking, either intermittent or continual, at whatever time or place, which interferes with an employee's functioning and performance in any respect of his or her job.

Aims

This Policy aims to clarify the Company's attitude to the use of alcohol or the use of drugs in work related situations and to provide systems of communication, education and training while maintaining confidentiality.

The aims are to:

- Prevent and / or reduce the incidence of alcohol / drug related problems in the workplace;
- Reduce the personal suffering of the employees concerned;
- Encourage the development of a climate that will remove the tendency to conceal or deny alcohol / drug related problems and give the employee and employer representatives the confidence to deal with them constructively;
- Ensure that performance and safety of others is not jeopardised by employees misusing alcohol and / or drugs.

Drugs

Taking of drugs or solvent misuse at work will not be tolerated unless the drugs are prescribed by a General Practitioner or other person qualified to prescribe such drugs.

Drugs which can be freely purchased over the counter from pharmacist and other reputable outlets such as supermarkets are also acceptable, provided that the dosage information is followed to the letter.

Employees should be aware however, that certain over-the-counter drugs and prescribed drugs have warnings on them which state that the consumption may cause drowsiness and warn against driving or operating machinery. If any of this type of drug is used at work, or prior to commencing work, and it is believed that the effects of the drug could still present themselves, the employee should make his or her Head of Department aware of this fact.

As a very rough guideline, the effects of drugs in the body may be expected to last for between four and six hours.

Should any persons be found to be supplying illegal drugs or drugs prescribed specifically for their own consumption to other persons, or are found to be misusing any solvents, this will be treated as gross misconduct and will be dealt with in accordance with the disciplinary procedure already in force.

Cannabis

The legal status of cannabis has not changed and its use by employees will not be tolerated. Cannabis affects people's long-term health, makes them relaxed and affects their concentration.

Some people who have tested positive for cannabis have claimed that they had been subject to 'passive smoking'. However there are tests available which can differentiate between passive inhalation and direct smoking.

If an employee suspects that cannabis is being used in the vicinity, he or she should consider moving away from the area to avoid inhaling the smoke. Employees should remember that if people near them are smoking cannabis,

they could be affected by the drug and therefore considered to be under its influence. Disciplinary action will be taken and the employee could be dismissed.

Alcohol

Whilst most people that consume alcohol are social drinkers and do not have a perceived addiction to alcohol, there are occasions when alcohol consumption may overlap into the workplace. As an example, consumption of excessive alcohol into the early hours on a day preceding a work day could result in alcohol remaining in the bloodstream at the time of work commencing.

Not only could this lead to prosecution from the Police (should the individual have driven a motor vehicle to work whilst under the influence of alcohol), but it could result in serious injury or death at work through lack of concentration or alertness etc. brought about by alcohol consumption.

Therefore the Company will not permit any person to consume alcohol during normal working hours, including during any breaks that are allowed, unless there are exceptional circumstances and express permission has been granted by a Director.

The types of exceptional circumstances that are envisaged are Company organised functions at which alcoholic beverages will be served.

If any employee is considered to be under the influence of alcohol, or if alcoholic odour is detected, the employee will be subject to the Company's disciplinary procedures. Where the employee’s continued attendance at work is considered to be in breach of Health & Safety legislation, he or she may be sent home without pay.

With regard to detecting alcohol and/or drugs by on-the-spot testing, there is a lesser burden of proof needed in employment law in order to dismiss an employee (gross misconduct) than there is in criminal law to convict a person for a drink/drug related offence. An employer is only required to conduct a fair and thorough investigation in order to make a decision to suspend or dismiss an employee. If the employer then believes that the employee is not safe to work (for example on machinery or vehicles), justification to suspend or dismiss may be regarded as fair.

Provisions

Any employee who has a drug or alcohol related problem should report this fact to a Director who will discuss the matter in strict confidence. The Company will adopt a sympathetic approach and, where appropriate, the employer will make suitable arrangements for counselling or advice. Such counselling or advice cannot continue if the behaviour of the employee is distressing, jeopardising the safety of others or jeopardising the reputation of the Company.

Employees who occasionally misuse alcohol, resulting in a breach of discipline or safety rules, are dealt with under the normal disciplinary process.

Where employees refuse the offer of referral to an appropriate agency, or where a course of treatment is discontinued before its satisfactory completion and the level of performance is still unsatisfactory, they will be subject to the normal disciplinary procedures that may ultimately result in their dismissal.

Managers or colleagues who cover up for an employee with an alcohol-related problem may be breaching their employer's statutory and common-law obligations under the Health and Safety at Work Act 1974.

24 EQUALITY OF OPPORTUNITY POLICY

Scope of Policy

The Company is an equal opportunity employer and is fully committed to a policy of treating all of its employees and job applicants equally.
The Company will take all reasonable steps to employ, train and promote employees on the basis of their experience, abilities and qualifications without regard to race, colour, ethnic origin, nationality, national origin, religion or belief, sex, sexual orientation, gender reassignment, age, marital or civil partnership status or disability. The Company will also take all reasonable steps to provide a work environment in which all employees are treated with respect and dignity and that is free of harassment based upon an employee's race, colour, ethnic origin, nationality, national origin, religion or belief, sex, sexual orientation, gender reassignment, age, marital or civil partnership status or disability. The Company will not condone any form of harassment, whether engaged in by employees or by outside third parties who do business with the Company, such as clients, customers, contractors and suppliers.

Employees have a duty to co-operate with the Company to ensure that this policy is effective in ensuring equal opportunities and in preventing discrimination, harassment or bullying. Action will be taken under the Company's disciplinary procedure against any employee who is found to have committed an act of improper or unlawful discrimination, harassment, bullying or intimidation. Serious breaches of this equal opportunities and dignity at work statement will be treated as potential gross misconduct and could render the employee liable to summary dismissal. Employees should also bear in mind that they can be held personally liable for any act of unlawful discrimination. Employees who commit serious acts of harassment may also be guilty of a criminal offence.

You should draw the attention of your line manager to suspected discriminatory acts or practices or suspected cases of harassment. You must not victimise or retaliate against an employee who has made allegations or complaints of discrimination or harassment or who has provided information about such

discrimination or harassment. Such behaviour will be treated as potential gross misconduct in accordance with the Company's disciplinary procedure.

The Company will also take appropriate action against any third parties who are found to have committed an act of improper or unlawful harassment against its employees.

Recruitment, advertising and selection

The recruitment process will be conducted in such a way as to result in the selection of the most suitable person for the job in terms of relevant experience, abilities and qualifications. The Company is committed to applying its equal opportunities policy statement at all stages of recruitment and selection.

Advertisements will encourage applications from all suitably qualified and experienced people. When advertising job vacancies, in order to attract applications from all sections of the community, the Company will, as far as reasonably practicable:

1. Ensure advertisements are not confined to those publications which would exclude or disproportionately reduce the numbers of applicants of a particular gender, sexual orientation, age, religion or racial group.
2. Avoid prescribing any unnecessary requirements which would exclude a higher proportion of a particular gender, sexual orientation, age, religion or racial group or which would exclude disabled job applicants.
3. Avoid prescribing any requirements as to marital or civil partnership status.
4. Where vacancies may be filled by promotion or transfer, they will be published to all eligible employees in such a way that they do not restrict applications from employees of any particular gender, sexual orientation, age, religion or racial group or from employees with a disability.

The selection process will be carried out consistently for all jobs at all levels. All applications will be processed in the same way. The staff responsible for short-listing, interviewing and selecting candidates will be clearly informed of the selection criteria and of the need for their consistent application. Person specifications and job descriptions will be limited to those requirements that are necessary for the effective performance of the job. Wherever possible, all applicants will be interviewed by at least two interviewers and all questions asked of the applicants will relate to the requirements of the job. The selection of new staff will be based on the job requirements and the individual's suitability and ability to do, or to train for, the job in question.

With disabled job applicants, the Company will have regard to its duty to make reasonable adjustments to work provisions, criteria and practices or to work premises in order to ensure that the disabled person is not placed at a substantial disadvantage in comparison with persons who are not disabled.

If it is necessary to assess whether personal circumstances will affect the performance of the job (for example, if the job involves unsociable hours or extensive travel), this will be discussed objectively, without detailed questions based on assumptions about race, colour, ethnic origin, nationality, national origin, religion or belief, sex, sexual orientation, gender reassignment, age, marital or civil partnership status, disability, children and/or domestic obligations.

Training and promotion

The Company will train all line managers in the Company's policy on equal opportunities and in helping identify discriminatory acts or practices or acts of harassment or bullying. Line managers will be responsible for ensuring they actively promote equal opportunity within the departments for which they are responsible.

The Company will also provide training to all employees to help them understand their rights and responsibilities in relation to dignity at work and what they can do to create a work environment that is free of bullying and harassment.

Where a promotional system is in operation, it will not be discriminatory and it will be checked from time to time to assess how it is working in practice. When a group of workers predominantly of one race, religion, sex, sexual orientation or age group or a worker with a disability appears to be excluded from access to promotion, transfer and training and to other benefits, the promotional system will be reviewed to ensure there is no unlawful discrimination.

Terms of employment, benefits, facilities and services

All terms of employment, benefits, facilities and service will be reviewed from time to time, in order to ensure that there is no unlawful discrimination on the grounds of race, colour, ethnic origin, nationality, national origin, religion or belief, sex, sexual orientation, gender reassignment, age, marital or civil partnership status or disability.

Equal pay

The Company is committed to equal pay in employment. It believes its male and female employees should receive equal pay for like work, work rated as equivalent or work of equal value. In order to achieve this, the Company will endeavour to maintain a pay system that is transparent, free from bias and based on objective criteria.

Bullying and harassment

Bullying is offensive or intimidating behaviour or an abuse or misuse of power which undermines or humiliates an employee.

Harassment occurs where, on the ground of an employee's race, colour, ethnic origin, nationality, national origin, religion or belief, sexual orientation, gender reassignment, age, marital or civil partnership status or disability, a person engages in unwanted conduct that:

- has the purpose of violating the employee's dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee; or
- is reasonably considered by the employee to have the effect of violating his or her dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee, even if this effect was not intended by the person responsible for the conduct.

Harassment also occurs where, related to either the employee's sex or that of another individual, a person engages in unwanted conduct that:

- has the purpose of violating the employee's dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee; or
- is reasonably considered by the employee to have the effect of violating their dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee, even if this effect was not intended by the person responsible for the conduct.

In this scenario, the employee does not need to be the subject of the unwanted conduct for harassment to have occurred - for example, the conduct could be directed at nobody in particular or at someone other than the employee, including someone of the opposite sex.

Sexual harassment (as opposed to harassment related to gender) occurs where a person engages in any form of unwanted conduct of a sexual nature that:

- has the purpose of violating the employee's dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee; or

- is reasonably considered by the employee to have the effect of violating his or her dignity at work, or of creating an intimidating, hostile, degrading, humiliating or offensive work environment for the employee, even if this effect was not intended by the person responsible for the conduct.

Conduct may be harassment whether or not the person intended to offend. Something intended as a “joke” or as “office banter” may offend another person. This is because different employees find different levels of behaviour acceptable and everyone has the right to decide for themselves what behaviour they find acceptable to them.

Behaviour which a reasonable person would realise would be likely to offend an employee will always constitute harassment without the need for the employee having to make it clear that such behaviour is unacceptable, for example, touching someone in a sexual way. With other forms of behaviour, it may not always be clear in advance that it will offend a particular employee, for example, office banter and jokes. In these cases, the behaviour will constitute harassment if the conduct continues after the employee has made it clear, by words or conduct, that such behaviour is unacceptable to him or her. A single incident can amount to harassment if it is sufficiently serious.

Harassment also occurs where, on the ground of the employee’s rejection of or submission to unwanted conduct of the kind specified above, a person treats the employee less favourably than he or she would treat him or her had he or she not rejected, or submitted to, the unwanted conduct.

Examples

Bullying and harassment may be verbal, non-verbal, written or physical.
Examples of unacceptable behaviour include, but are not limited to, the following:

- unwelcome sexual advances, requests for sexual favours, other conduct of a sexual nature
- subjection to obscene or other sexually suggestive or racist comments or gestures
- the offer of rewards for going along with sexual advances or threats for rejecting sexual advances
- jokes or pictures of a sexual or racial nature
- demeaning comments about an employee’s appearance
- questions about a person’s sex life
- the use of nick names related to an employee’s sex, sexual orientation, gender reassignment, race, religion, age or disability
- picking on or ridiculing an employee

- isolating an employee or excluding him or her from social activities or relevant work-related matters.

Reporting complaints

All allegations of discrimination or harassment will be dealt with seriously, confidentially and speedily. The Company will not ignore or treat lightly grievances or complaints of discrimination or harassment from members of a particular race, colour, ethnic origin, nationality, national origin, religion or belief, sex, sexual orientation or age or from employees who have undergone gender reassignment, are married, have entered into a civil partnership or have a disability.
With cases of harassment, while the Company encourages employees who believe they are being harassed to notify the offender (by words or by conduct) that his or her behaviour is unwelcome, the Company also recognises that actual or perceived power and status disparities may make such confrontation impractical.
If you wish to make a complaint of discrimination or harassment, whether against the Company, a fellow employee or a third party, you should follow the following steps:

1. First of all, report the incident of discrimination or harassment to your line manager. If you do not wish to speak to your line manager, you can instead speak to an alternative manager or to a member of the Human Resources Department.
2. Such reports should be made promptly so that investigation may proceed and any action taken expeditiously.
3. All allegations of discrimination or harassment will be taken seriously. The allegation will be promptly investigated and, as part of the investigatory process, you will be interviewed and asked to provide a written witness statement setting out the details of your complaint. Confidentiality will be maintained during the investigatory process to the extent that this is practical and appropriate in the circumstances. However, in order to effectively investigate an allegation, the Company must be able to determine the scope of the investigation and the individuals who should be informed of or interviewed about the allegation. For example, the identity of the complainant and the nature of the allegations must be revealed to the alleged harasser or discriminator so that he or she is able to fairly respond to the allegations. The Company reserves the right to arrange for another manager to conduct the investigation other than the manager with whom you raised the matter.
4. Once the investigation has been completed, you will be informed in writing of the outcome and the Company's conclusions and decision as soon as

possible. The Company is committed to taking appropriate action with respect to all complaints of discrimination or harassment which are upheld.

5. You will not be penalised for raising a complaint, even if it is not upheld, unless your complaint was both untrue and made in bad faith.

6. If your complaint is upheld and the harasser or discriminator remains in the Company's employment, the Company will take all reasonable steps to ensure that you do not have to continue working alongside him or her if you do not wish to do so. The Company will discuss the options with you.

7. If your complaint is not upheld, arrangements will be made for you and the alleged harasser or discriminator to continue or resume working and to repair working relationships.

Alternatively, you may, if you wish, use the Company's grievance procedure to make a complaint.

Any employee who is found to have discriminated against or harassed another employee in violation of this policy will be subject to disciplinary action under the Company's disciplinary procedure. Such behaviour may be treated as gross misconduct and could render the employee liable to summary dismissal. In addition, line managers who had knowledge that such discrimination or harassment had occurred in their departments but who had taken no action to eliminate it will also be subject to disciplinary action under the Company's disciplinary procedure.

Monitoring equal opportunity and dignity at work

The Company will regularly monitor the effects of selection decisions and personnel and pay practices and procedures in order to assess whether equal opportunity and dignity at work are being achieved. This will also involve considering any possible indirectly discriminatory effects of its working practices. If changes are required, the Company will implement them. The Company will also make reasonable adjustments to its standard working practices to overcome barriers caused by disability.

25 DIGNITY AT WORK POLICY

Policy statement

The Company seeks to provide a work environment in which all employees are treated with respect and dignity and that is free from harassment and bullying based upon age, disability, gender reassignment, race (including colour, nationality and ethnic or national origins), religion or belief, sex or sexual orientation. In this policy, these are known as the "protected characteristics".

Employees have a duty to co-operate with the Company to make sure that this

policy is effective in preventing harassment or bullying. Action will be taken under the Company's disciplinary procedure against any employee who is found to have committed an act of improper or unlawful harassment, bullying or intimidation. Serious breaches of this dignity at work policy statement will be treated as potential gross misconduct and could render the employee liable to summary dismissal. Employees should bear in mind that they can be held personally liable for any act of unlawful harassment. Employees who commit serious acts of harassment may also be guilty of a criminal offence.

All employees are responsible for conducting themselves in accordance with this policy. The Company will not condone or tolerate any form of harassment, bullying or intimidation, whether engaged in by employees or by outside third parties who do business with the Company, such as clients, customers, contractors and suppliers.

You should draw the attention of your line manager to suspected cases of harassment, bullying or intimidation. You must not victimise or retaliate against an employee who has made allegations or complaints of harassment or who has provided information about such harassment. Such behaviour will be treated as potential gross misconduct in accordance with the Company's disciplinary procedure. You should support colleagues who suffer such treatment and are making a complaint.

The Company will also take appropriate action against any third parties who are found to have committed an act of improper or unlawful harassment, bullying or intimidation against its employees.

This policy covers harassment, bullying and intimidation both in the workplace and in any work-related setting outside the workplace, for example during business trips, at external training events or at work-related social events.

Bullying and harassment

Bullying is offensive or intimidating behaviour or an abuse or misuse of power which undermines or humiliates an employee.

An employee unlawfully harasses another employee if they engage in unwanted conduct related to a protected characteristic, and the conduct has the purpose or effect of violating the other employee's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for that other employee. An employee also unlawfully harasses another employee if they engage in unwanted conduct of a sexual nature, and the conduct has the purpose or effect of violating the other employee's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for that other employee.

Finally, an employee unlawfully harasses another employee if they or a third party

engage in unwanted conduct of a sexual nature or that is related to gender reassignment or sex, the conduct has the purpose or effect of violating the other employee's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for that other employee, and because of that other employee's rejection of or submission to the conduct, they treat that other employee less favourably than they would treat them if they had not rejected, or submitted to, the conduct.

The unwanted conduct will still amount to harassment if it is based on the protected characteristic of a third party with whom the employee is associated and not on the employee's own protected characteristic, or if it was directed at someone other than the employee, or even at nobody in particular, but they witnessed it. In addition, harassment can include cases where the unwanted conduct occurs because it is perceived that an employee has a particular protected characteristic, when in fact they do not.

Conduct may be harassment whether or not the person intended to offend. Something intended as a "joke" or as "office banter" may offend another person. This is because different employees find different levels of behaviour acceptable and everyone has the right to decide for themselves what behaviour they find acceptable to them.

Behaviour which a reasonable person would realise would be likely to offend an employee will always constitute harassment without the need for the employee having to make it clear that such behaviour is unacceptable, for example, touching someone in a sexual way. With other forms of behaviour, it may not always be clear in advance that it will offend a particular employee, for example, office banter and jokes. In these cases, the behaviour will constitute harassment if the conduct continues after the employee has made it clear, by words or conduct, that such behaviour is unacceptable to him or her. A single incident can amount to harassment if it is sufficiently serious.

Examples

Bullying and harassment may be verbal, non-verbal, written or physical. Examples of unacceptable behaviour include, but are not limited to, the following:

- unwelcome sexual advances, requests for sexual favours, other conduct of a sexual nature
- subjection to obscene or other sexually suggestive or racist comments or gestures, or other derogatory comments or gestures related to a protected characteristic
- the offer of rewards for going along with sexual advances or threats for rejecting sexual advances
- jokes or pictures of a sexual, sexist or racial nature or which are otherwise

derogatory in relation to a protected characteristic

- demeaning comments about an employee's appearance
- questions about an employee's sex life
- the use of nicknames related to a protected characteristic whether made orally or by e-mail
- picking on or ridiculing an employee because of a protected characteristic
- isolating an employee or excluding him or her from social activities or relevant work-related matters because of a protected characteristic.

Reporting complaints

All allegations of harassment, bullying or intimidation will be dealt with seriously, confidentially and speedily. The Company will not ignore or treat lightly grievances or complaints of harassment from employees.

While the Company encourages employees who believe they are being harassed or bullied to notify the offender (by words or by conduct) that his or her behaviour is unwelcome, the Company also recognises that actual or perceived power and status disparities may make such confrontation impractical. In the event that such informal direct communication is either ineffective or impractical, or the situation is too serious to be dealt with informally, you should follow the procedure set out below.

If you wish to make a complaint of harassment, bullying or intimidation, whether against a fellow employee or a third party, such as a client, customer, contractor or supplier, you should follow the following steps:

1. First of all, report the incident of harassment to your line manager. If you do not wish to speak to your line manager, you can instead speak to an alternative manager or to a member of the Human Resources Department.

2. Such reports should be made promptly so that investigation may proceed and any action taken expeditiously.

3. All allegations of harassment will be taken seriously. The allegation will be promptly investigated and, as part of the investigatory process, you will be interviewed and asked to provide a written witness statement setting out the details of your complaint. Confidentiality will be maintained during the investigatory process to the extent that this is practical and appropriate in the circumstances. However, in order to effectively investigate an allegation, the Company must be able to determine the scope of the investigation and the individuals who should be informed of or interviewed about the allegation. For example, the identity of the complainant and the nature of the allegations must be revealed to the alleged harasser so that he or she is able to fairly respond to the allegations. The Company reserves the right to arrange for another

manager to conduct the investigation other than the manager with whom you raised the matter.

4. Once the investigation has been completed, you will be informed in writing of the outcome and the Company's conclusions and decision as soon as possible. The Company is committed to taking appropriate action with respect to all complaints of harassment which are upheld. If appropriate, disciplinary proceedings will be brought against the alleged harasser.

5. You will not be penalised for raising a complaint, even if it is not upheld, unless your complaint was both untrue and made in bad faith.

6. If your complaint is upheld and the harasser remains in the Company's employment, the Company will take all reasonable steps to ensure that you do not have to continue working alongside him or her if you do not wish to do so. The Company will discuss the options with you.

7. If your complaint is not upheld, arrangements will be made for you and the alleged harasser to continue or resume working and to repair working relationships.

Alternatively, you may, if you wish, use the Company's grievance procedure to make a complaint of harassment.

Disciplinary action

Any employee who is found to have harassed another employee in violation of this policy will be subject to disciplinary action under the Company's disciplinary procedure. Such behaviour may be treated as gross misconduct and could render the employee liable to summary dismissal. In addition, line managers who had knowledge that such harassment had occurred in their departments but who had taken no action to eliminate it will also be subject to disciplinary action under the Company's disciplinary procedure.

Training

The Company will train all line managers in the Company's policy on dignity at work and in helping them identify and deal effectively with harassment, bullying or intimidation. Line managers will be responsible for ensuring they actively promote dignity at work within the departments for which they are responsible.

The Company will also provide training to all employees to help them understand their rights and responsibilities in relation to dignity at work and what they can do to create a work environment that is free from harassment, bullying and intimidation.

26 COMPANY VEHICLE POLICY

Usage

All employees must:

- Make sure their driving licence is up to date.
- Notify the Company immediately of any disabilities which may affect their driving ability.

Only authorised members of staff may drive the Company's vehicles. Private use of such vehicles requires additional approval. Authorisation will only be given on possession and production of a valid driving licence, which will be subject to inspection on an annual basis.

Authorised members of staff are permitted to use a designated Company vehicle for reasonable private use of a normal domestic nature. However, where the vehicle is to be taken for personal reasons outside the United Kingdom, prior approval must first be obtained from a Director. For any travel outside the UK (whether for personal or Company reasons) it is the driver's responsibility to notify the Company's insurers at least 2 weeks before he or she is expecting to travel to ensure appropriate insurance cover is in place. The driver will be responsible for all and any additional insurance costs as a result of any premium levied by the Company's insurers in respect of personal travel abroad. The driver must also be able to produce prior evidence that his or her insurance cover will allow for returning the Company vehicle back to his or her home address if it becomes either immobile or unsafe to drive.

Vehicles are insured for use by anyone over the age of 25.

Employees may not carry unauthorised passengers in Company vehicles, nor may the vehicles be hired out or used for personal gain.

Fuel

Where an employee is provided with a Company Fuel Card, the Card is to be used exclusively for business use only, and in accordance with the laid down procedure, at the designated garages only.

However the Company accepts that in certain exceptional and unavoidable circumstances it may be necessary to purchase petrol on either a Company credit card or by the individual. In such cases any transaction must be brought to the attention of the Company and substantiated by a valid and appropriate receipt. The Company reserves the right to make a deduction from pay where it believes that an employee has either failed to follow the correct procedure or where the Company believes that a Company card has been used fraudulently.

The employee must return the Fuel Card to the Company immediately upon request and on termination of his or her employment.

If authorisation is given for the use of a private vehicle on Company business, the Company will pay for fuel for the business use in full by way of a mileage allowance.

The rate will be £0-40 per mile and must be supported by a fully completed Expense Form.

Parking and Congestion Charges

Parking fees incurred for legitimate business purposes will be reimbursed to the individual in full immediately on production of a receipt.

Parking fines incurred by any individual whether on business or not will **NOT** be paid by the Company.

Payment within the published time limits for driving within Congestion Charging Zones is the responsibility of each individual driver. Various payment methods are available for this purpose.

Payments made by individual drivers will be reimbursed immediately.

Penalties incurred for non-payment are the responsibility of the driver.

Maintenance

When driving a Company vehicle, employees must ensure that the vehicle is in a clean and roadworthy condition at all times. When an employee is allocated a new / different company vehicle, the driver will be expected to sign a check sheet regarding the vehicle standard. All routine vehicle inspections, including oil and water levels, tyre pressure and tread depth, brake and power steering fluid reservoirs and lights and indicators, should be carried out on a daily basis and any defects must be reported without delay.

When a vehicle is due to be serviced, it is the employee's responsibility to notify the Club Secretary when the mileage on a vehicle he or she is driving is 2000 miles less than the required mileage band for the next service. If an employee is in any doubt he or she should consult the Club Secretary.

Security

Security measures must be followed at all times for the safe keeping of the vehicle and its contents, i.e. when left unattended for any period of time (this includes a garage forecourt) the vehicle must be locked securely, items of value must be removed and other items not left in open view.

Incidents

On the occasion of any incident involving a Company vehicle, the employee must make a full, honest and written report of the occurrence whether or not personal injury or vehicle damage is involved.

All such incidents will be investigated and. where an investigation shows an

employee to be at fault, he or she may be subject to disciplinary action. An excessive number of incidents will result in dismissal.

Where personal injury has occurred the employee must declare the name and policy number of the Company's insurers.

The employee must immediately report to his or her Manager any type of damage sustained to the vehicle, no matter how minor, otherwise the company from whom the vehicles are leased may levy a penalty charge.

No statements must be made to the police as a result of any incident involving an employee's Company vehicle without first discussing the matter with a Director of the Company. This is particularly important in cases involving death or injury.

Violations and Convictions

Traffic violations include:

- Parking.
- Speeding.
- Accidents.
- Use of mobile telephones whilst in charge of the vehicle.

When driving Company vehicles employees must abide by the relevant appropriate statutory regulations at all times. The Company does not condone traffic violations of any description and accepts no responsibility for them by any individual whether incurred on Company business or otherwise. Payment of fines is the responsibility of the vehicle user.

All employees must notify the Company immediately of any endorsements received.

An employee must immediately report to his or her Head of Department any type of driving conviction or summons which may lead to a conviction. All fines resulting from convictions or other offences are the employee's own responsibility. If prompt payment is not made the Company will deduct the amount from the employee's pay and ensure that due payment is made.

The Company will take a serious view of continuous exceeding of speed limits.

Driving bans

Should an individual receive a driving ban through their own actions and as a result be unable to fulfil the terms of their contract of employment, the following shall apply:

Ban of up to 28 days:	All outstanding holiday entitlement must be taken with any balance taken as unpaid leave.
Ban of over 28 days:	Summary dismissal.

Before taking any decision to dismiss, the Company will discuss the matter with you to allow you to make suggestions as to how the job could be carried out while your license is suspended.

Both of these are at the discretion of the directors.

Other considerations

Statutory and employer's regulations regarding the recording of daily mileage, journey undertaken and actual driving hours must be complied with.

Personal auxiliary equipment must not be fitted in or on a Company vehicle without management approval.

In order to maintain its business use, the right is reserved to recover any issued Company vehicle from its nominated driver in the event of an absence from work for any reason.

Where any damage to, or loss from, a Company vehicle is due to gross negligence or lack of care on the part of an employee, the Company reserves the right to insist on the employee:

- Rectifying all or part of the damage, or
- Paying for the replacement cost of any item at his or her own expense, or
- Being responsible for the insurance excess.

If the employee does not carry this out appropriately and timely, the Company reserves the right to make a deduction from his or her pay to an amount equal to the damage or loss incurred by the Company.

Smoking is not permitted in any Company vehicles.

27 HEALTH & SAFETY POLICY

It is the policy of Blundells Hill Golf Club Limited to provide and maintain a healthy and safe working environment and to comply with the terms of the Health and Safety at Work etc Act 1974 and subsequent legislation.

Under Section 7 of the Health and Safety at Work etc Act it is the duty of every employee while at work:

a) To take reasonable care for the health and safety of himself and of other persons who may be affected by his or her acts or omissions at work, and
b) As regards any duty or requirement imposed on his or her employer, to co-operate with him so far as is necessary to enable that duty or requirement to be performed or complied with.

Information on the Company's Health and Safety Policy, Arrangements and Responsibilities is described in a separate document.

Any breach to these Health and Safety arrangements may result in disciplinary action.

28 SMOKE-FREE POLICY

The Company operates a no smoking policy throughout its premises at all times, with no exceptions to staff or clients.

This policy has been developed to protect all employees, service users, clients and visitors from exposure to second-hand smoke and to assist compliance with the Health Act 2006.

Exposure to second-hand smoke increases the risk of lung cancer, heart disease and other serious illnesses. Ventilation or separating smokers and non-smokers within the same airspace do not completely stop potentially dangerous exposure.

It is the policy of Blundells Hill Golf Club Limited that all its workplaces are smoke-free and all employees have a right to work in a smoke-free environment. Smoking is prohibited in all enclosed and substantially enclosed premises in the workplace.

This includes company vehicles. This policy applies to all employees, consultants, contractors, clients and visitors.

Overall responsibility for policy implementation and review rests with the Managing Director. However, all staff are obliged to adhere to, and support the implementation of the policy.

Appropriate ‘no-smoking’ signs will be clearly displayed at the entrances to and within the premises, and in all smoke-free vehicles.

Blundells Hill Golf Club Limited’s Disciplinary Procedure will be followed if a member of staff does not comply with this policy. Those who do not comply with the smoke-free law may also be liable to a fixed penalty fine and possible criminal prosecution.

The National Health Service offers a range of free services to help smokers give up. Visit gosmoke-free.co.uk or call the NHS Smoking Helpline on 0800 169 0 169 for details. Alternatively smokers can text ‘GIVE UP’ and their full postcode to 88088 to find their local NHS Stop Smoking Service.

29 STRESS POLICY

Introduction

Blundells Hill Golf Club Limited is committed to protecting the health, safety and welfare of its employees. It recognises that workplace stress is a health and safety issue and acknowledges the importance of identifying and reducing workplace stressors.

Most people will suffer from stress at some time during their life. Stress can provide motivation and achievement. However, if someone becomes over-stressed a range of medical symptoms may appear together with low performance, irritability and depression etc. Stress can be caused by environmental factors such as noise, heat, humidity, cold or lighting as well as work relationships, work loads and tight deadlines and where routine tasks may produce major problems.

This policy applies to everyone in the Company. Managers are responsible for its implementation and the Company is responsible for providing the necessary resources.

Definition of Stress

The Health and Safety Executive define stress as “the adverse reaction people have to excessive pressure or other types of demand placed on them”. This makes an important distinction between pressure, which can be a positive state if managed correctly, and stress which can be detrimental to health.

Policy

The Company will identify all workplace stressors and conduct risk assessments to eliminate stress or control the risks from stress. These risk assessments will be regularly reviewed.

The Company will consult with Safety Representatives on all proposed action relating to the prevention of workplace stress.

The Company will provide training for all managers and supervisory staff in good management practices.

The Company will provide confidential counselling for staff affected by stress caused by either work or external factors.

The Company will provide adequate resources to enable managers to implement the Company’s agreed stress management strategy.

Responsibilities

The responsibilities of the Directors are to:

- Give guidance to managers on the stress policy.
- Assist in monitoring the effectiveness of measures to address stress by collating sickness absence statistics.
- Advise managers and individuals on training requirements.
- Provide continuing support to managers and individuals in a changing environment and encourage referral to occupational workplace counsellors where appropriate.

The responsibilities of Managers are to:

- Conduct and implement recommendations of risks assessments within their jurisdiction.
- Ensure good communication between management and staff, particularly where there are organisational and procedural changes.
- Ensure all staff are fully trained to discharge their duties.
- Ensure all staff are provided with meaningful developmental opportunities.
- Monitor workloads to ensure that personnel are not overloaded.
- Monitor working hours and overtime to ensure that all staff are not overworked.
- Monitor holidays to ensure that the staff are taking their full entitlement.
- Attend training as requested in good management practice and health and safety.
- Ensure that bullying and harassment is not tolerated within their jurisdiction.
- Be vigilant and offer additional support to a member of staff who is experiencing stress outside work, e.g. bereavement or separation.

The responsibilities of Occupational Health and Safety Advisors are to:

- Provide specialist advice and awareness training on stress.
- Train and support managers in implementing stress risk assessments.
- Support individuals who have been off sick with stress and advise them and their management on a planned return to work.
- Refer to workplace counsellors or specialist agencies as required.
- Monitor and review the effectiveness of measures to reduce stress.
- Inform the employer and the health and safety committee of any changes and developments in the field of stress at work.

The responsibilities of each Employee are to:

- Raise issues of concern with their Safety Representative, line manager or occupational health.
- Accept opportunities for counselling when recommended.

Function of Safety Representatives

In order to perform their duties effectively, Safety representatives must:

- Be meaningfully consulted on any changes to work practices or work design that could precipitate stress.
- Be able to consult with members on the issue of stress, including conducting any workplace surveys.
- Be involved in the risk assessment process.
- Be allowed access to collective and anonymous data regarding the workforce.

- Be provided with paid time away from normal duties to attend any reasonable training relating to workplace stress.
- Conduct joint inspections of the workplace regularly to ensure that environmental stressors are properly controlled.

Role of the Safety Committee

The Safety Committee will perform a pivotal role in ensuring that this policy is implemented. They will oversee monitoring of the efficacy of the policy and other measures to reduce stress and promote workplace health and safety.

30 QUALITY POLICY

Blundells Hill Golf Club Limited is committed to provide a golf course of the highest standard and to provide services of high quality and reliability to its Members and clients. An important element of this Policy is to maintain and improve the Company's facilities and services to provide continued client satisfaction.

Adherence to the Quality Policy involves all of Blundells Hill Golf Club Limited's activities and employees. All employees are responsible for the quality of their own work and are committed to participate in the operation of the Company's procedures and the provision of excellent services.

31 ENVIRONMENT POLICY

As an organisation, Blundells Hill Golf Club Limited is aware that it has an impact on the environment. It is the Company's Policy to provide a high quality golfing facility while maintaining an environmentally sensitive ecological policy.

The Company is committed to environmental improvements and a reduction of its environmental impact. The Company is also committed to:

- Meeting all relevant statutory requirements of environmental legislation and where no standards exist, setting their own high standards.
- Training staff in the Company's environmental management procedures and other environmental matters.
- Involving and informing club members regarding ongoing environmental management of the golf course, and encouraging members to take an interest in the well-being of the course and its wildlife.

- Maximising the quality of the playing area, based on environmentally sound procedures and practices.
- Conserving and enhancing the biodiversity of the golf course through ongoing, informed management of species and habitats.
- Preventing pollution by reducing energy, water and chemical use, and by using more environmentally friendly chemicals.
- Minimising the amount of waste produced by the Club and ensuring that all handling and disposal practices meet with best environmental practice, with re-use and recycling of materials as appropriate.
- Ensuring that actions are evaluated with regard to their potential impact on the character of the golf course and its surrounds.
- Ensuring that staff and Club Members are aware of this policy by displaying it on notice boards around the site and making this Policy available to other interested parties

Adherence to this Environmental Policy involves all of Blundells Hill Golf Club Limited's activities and employees.

32 GENERAL CONDITIONS OF EMPLOYMENT

The following general points all form part of each employee's Contract of Employment.

Acts Prejudicial to the Company

Any acts prejudicial to the Company that are not specifically covered by an employee's Contract of Employment or this Staff Handbook will be dealt with on their own merit.

Appraisals

Each employee's performance may be monitored and reviewed on a quarterly basis through an appraisal with his or her department manager. This is an opportunity to discuss past and future progression, the employee's achievements, to compare his or her performance against targets and to agree and discuss targets for the following quarter.

Bad Weather Conditions

If an employee's job involves working outside in all weather conditions there are likely to be occasions when, due to extremes of bad weather, it is not possible for the job to be done. In these circumstances and where alternative work is not available, the employee may be subject to temporary lay-off without normal pay until the weather conditions improve. The terms and conditions of the statutory guarantee payment scheme will apply.

- No guarantee to provide a continuous standard working week.
- Decision to cease work will be made by a Director.

Bereavement Leave

Paid leave of absence **may** be made at the discretion of a Director in the case of bereavement. The following are the maximum numbers of paid days the Company will allow:

Three (3) days:

- Spouse.
- Partner.
- Child.
- Parent.
- Brother/Sister.

One (1) day:

- Grandparent.
- Grandchild.
- In-Laws.
- Uncle/Aunt.
- Cousin.
- Nephew/niece.
- Close Friend.

Outstanding holiday entitlement should be used to provide payment for bereavement leave beyond that which may be authorised.

Buying or Selling of Goods

Employees are not allowed to buy or sell goods on their own behalf on Company premises without prior permission. However, where permission is given the employee must ensure that any such activities do not cause any disruption to the working day.

Cash Handling

If the job requires that an employee handles cash, he or she should exercise caution and security and hand the money into the Company as quickly as possible.

Cash Handling / Petty Cash

If the job requires an employee to be entrusted with money and merchandise, he or she must exercise due care and obey the following rules:

1 The till drawer must be kept locked at all times and cash must not be left unattended.

2 At the close of business each day, all till monies are to be removed and locked away in the safe. A £100 float will be left in one secure till.

3 Full details of every sale must be entered into the cash register.

4 The till drawer must be closed after each transaction.

5 If an error is made when using the till, immediate assistance must be obtained from the Head of Department.

6 An employee is not allowed to complete refunds of any kind without permission from his or her Head of Department.

7 Cheque payments should be supported by a current valid guarantee card. The customer's card number must be entered on the reverse side of the cheque together with the employee's own initials.

8 For every credit card transaction, checks must be made to ensure the signature on the card matches the signature on the credit card slip and that the card is not out of date.

9 Employees who are uncertain about any transaction must seek further advice and guidance before the transaction is completed.

10 The till drawer must not be opened unless a transaction is being carried out. If there is a need to open the till drawer, i.e. as a result of incorrect change being given, it must only be done by a Manager who must initial the till roll to confirm his or her presence and approval.

11 The Manager will cash up daily and balance the tills leaving them ready in the safe for the following day's business.

The above till rules are easy to follow and are designed to safeguard everyone operating the cash register. They must be respected and any failure in an employee's duty to do so is likely to result in disciplinary action including possible termination of employment.

Change of Address and Telephone Number

Employees who change their address and/or contact telephone number must notify the Club Secretary without delay.

Collections

The Company recognises the value of Charity Collections and encourages this type of activity. However, permission to make the collection must be sought from a Director and care must be taken not to make employees feel harassed or obliged into donating.

Company Collections

Whilst the Company appreciates that employees may wish to present their colleagues with gifts on a collection basis from time to time, it believes collections

for such gifts should be controlled. They may be undertaken, therefore, only when a member of Management has given authorisation.

Compassionate Leave

Compassionate Leave with pay for periods not exceeding 2 weeks may be granted by a Director in exceptional circumstances only.

Details regarding leave in the case of bereavement are referred to under ‘Bereavement Leave' above.

Confidentiality

You must not, during or after the period of your employment, divulge to any outside body any trade secrets, recipes or confidential information about the business or any of its customers. This includes supplier and customer details and all pricing lists.

Personnel shall not remove from the place of their employment any documentation of any description, nor take copies of such documentation, for their personal use or the use of a competitor or third party either during their employment or on termination of their employment.

Any information provided by the Company to employees will be regarded as confidential unless it is of a type that would be:

(a) Freely available to the general public.
(b) Freely available to members of the Company's trade or profession.

Consultants or Contractors (Private Use of)

No employee is to gain special advantage by virtue of their position within the Company. For example it is not acceptable for an employee to use, on a personal basis, the services of a consultant, contractor, professional adviser or other individual without obtaining specific prior written authority from a Director. Once approval has been obtained the employee must be able to substantiate any work carried out by way of a formal receipt. Failure to obtain the appropriate written approval or a formal receipt could lead to disciplinary action being taken.

Fire and Evacuation Procedures

In the event of the fire alarm being sounded the Duty Manager will silence the alarm and dispatch a fire team to investigate. If a fire is found the team will report back to the Duty Manager and the alarms will be sounded for the second time. When this happens everybody should evacuate the building immediately and proceed without delay to the allocated Fire Assembly Point. Nobody should attempt to go back to collect any personal items.

As employees make for the nearest exit, they should close all windows and doors. Fire Officers are appointed for each department to supervise the evacuation of the premises and any instructions they give must be followed.

Any further information on local fire regulations can be found on the main notice boards and in the Company Health and Safety Manual.

First Aiders

As part of the Company's commitment to the continued health and safety of its employees, official First Aiders are appointed. For an up to date list of First Aiders within the Company please refer to the Staff Notice Board. Their duties are to treat cases needing First Aid, when required to do so, ensuring that a record of any such treatment is kept in a First Aid/Accident Record Book.

Gambling

Gambling is not permitted on the Company's premises.

Gifts / Hospitality

Blundells Hill Golf Club Limited discourages the acceptance of gifts or hospitality, other than items or gestures of a nominal nature/value. However, there may be occasions when an employee offered gifts or hospitality and in such instances he or she must declare it immediately to a Director. Employees are reminded that corruptly accepting any gifts or hospitality can lead to dismissal and possible criminal proceedings.

Housekeeping

From the point of view of safety and appearance, all work(ing) and rest areas must be kept clean and tidy at all times. Employees have a duty to maintain their Working Environment in order to achieve a Good Housekeeping Policy.

Ideas and Suggestions

Employees are encouraged to submit ideas for improving the health, safety, welfare and efficiency of the Company.

Jury Service / Court Attendance

If an employee is required to attend Court as a Juror or is subpoenaed as a witness, he or she must inform their manager immediately. There are allowances paid by the Court to cover loss of earnings to compensate people during their absence from work. The balance of the employee's basic pay **will not** be made up by the Company.

No payments will be made to an employee requiring time off work to answer civil or criminal charges.

Keys

If an employee is given a set of door keys for the building, they must be kept safely at all times. The keys must not be left unattended at any time and, when asked to lock up, the employee must ensure that all doors and windows in the Club House/Function Room are securely locked and any other final checks

followed to ensure the safety of the building and equipment. The employee must return all such keys on his or her termination of employment or on request of a Director.

Letters of Reference

Building Societies etc. may apply to the Company for letters of reference regarding employees. Reference enquiries by other employers may be made to a Director whilst someone is currently employed, or for up to three years after he or she has left. Open letters of reference will not normally be given.

Mobile Phones

The Company provides mobile phones to certain employees for business use.

This policy provides guidance on the use of mobile phones and employees must exercise due care and regard for the following rules:

1.1 The Company reserves the right to make a deduction from pay when it considers that personal use of a business mobile phone is excessive, unreasonable or inappropriate. In these circumstances the personal calls will be invoiced to the holder of the mobile phone and an equivalent amount of the cost of the calls will be deducted from pay. Persistant abuse will subject the employee to action under the disciplinary procedure.

1.2 For all staff other than Greenkeepers, personal mobile phones must be kept switched off whilst employees are working.

1.3 Mobile phones must not be used whilst employees are working on site and must be kept switched off whilst they are using machinery or if they are working at height. It is the employee's responsibility to ensure that any other customer site rules, applicable to the use of mobile phones, are observed.

Use of Mobile Telephones when Driving.

1.4 The actual use of the telephone hand set by the driver whilst the engine to the vehicle is running is contrary to the basic requirement of the Highway Code. Any such use may lead to prosecution by the Police Authority.

1.5 Employees are not permitted to use a mobile phone while driving on Company business under any circumstances. This includes when the vehicle is stationary with the engine running. Using a mobile phone whilst driving, whether or not the phone is on hands free, is potentially dangerous to the driver, other road users and pedestrians. The Company will not accept any responsibility for liabilities arising from a failure to comply with this policy.

1.6 The employee's phone must be kept switched off whilst he or she is driving and the voicemail facility should be utilised, unless a work colleague is travelling as a passenger and is able to use the phone.

1.7 When an outgoing call is being made, employees should find a safe place to stop before making the call and their vehicle must remain stationary for the duration of the call.

1.8 Employees should be aware of potential theft when stopping at a set of traffic lights, or when the car is parked. Telephones must therefore be concealed out of temptation of thieves. When a vehicle is left unattended the phone should be removed.

1.9 Employees must ensure that all mobile telephone equipment is turned off when refuelling a car or waiting on a filling station forecourt.

The above rules are easy to follow and are designed to safeguard employees. The rules must be respected and any failure to do so will result in disciplinary action, including possible termination of employment.

Notice Board(s)

Notice boards are situated throughout the Company and are used to communicate important information to all employees, such as vacancies, new events and other significant details of general interest. All private material should be authorised by the employee's Manager before being displayed on a Company notice board.

Parking

At any time that a vehicle is parked on Company premises it is left entirely at the driver's risk and no liability for any damage will be accepted by the Company.

Personal Mail

All mail sent to the Company is regarded as being addressed to the Company and will be opened. Personal mail must not be sent care of the Company unless prior approval has been given by Management.

Employees' Property

No liability is accepted for any loss of, or damage to, employees' property brought onto the premises. Employees are requested not to bring personal items of value on to the premises and, in particular, not to leave any items overnight. Employees are advised to ensure that personal possessions are covered by their own insurance policy.

Personal Telephone Calls

Telephones are provided for essential aspects of the business. Private outgoing telephone calls are only allowed with prior permission. All incoming personal calls must be kept to a minimum.

Protective Work Wear

Where protective work wear is appropriate for their place of work, employees are

expected to arrive on site with any personally allocated protective work wear, e.g.

- Hard helmet
- Protective high-visibility coat or waistcoat
- Protective safety boots
- Ear defenders
- Goggles
- Gloves

These form the basic protective personal equipment needed. However it may be necessary for an employee to wear additional protective equipment made available by the Company which is appropriate for the job being undertaken.

If an employee arrives at work without any, or part, of the necessary protective work wear or equipment, he or she will not be permitted onto site. The employee shall not be entitled to payment for any time lost as a result of his or her failure to have the proper work wear or equipment needed.

Where appropriate, the safety and protective clothing provided must be worn.

Subject to employees returning old, damaged or worn items to the Company, protective work wear provided by the Company will be replaced on a fair wear and tear basis.

Where the Company considers that work wear provided to a employee has suffered excessive wear, tear or damage resulting from use outside of the employee's working hours with the Company, or from use during secondary employment, the right is reserved not to pay for the replacement of such items and to insist that the employee covers the full cost of any new items required.

Redundancy

Should circumstances arise where redundancy is seen to be a possibility, the first steps will be to:

- Reduce overtime to a workable minimum.
- Restrict recruitment.
- Investigate measures such as short-time working and / or lay off (without normal pay) as a means of avoiding redundancies.

If redundancies cannot be avoided, consideration will be given to requesting applications for voluntary redundancy.

If the selection of employees for redundancy becomes necessary, the following will be considered:

- Previous work experience and the ability to transfer to other jobs.
- Previous disciplinary, absence, timekeeping and conduct records.
- Previous job performance and the ability to be re-trained.
- Length of service.

- Reliability and co-operation.

Due weight will be given to each of the above factors. Only if the final weighted score of the above was equal would the "last in first out" principle apply.

At all times in a redundancy situation, the overriding consideration will be the future needs and viability of the business.

Religious and Political Activities

The Company has no religious or political bias and does not condone any activity that is offensive to others or causes discomfort to an individual or disruption to working practices. The Company is not prepared to allow such activities on the premises.

Right of Search

The Company has the right to carry out random checks on the identity, persons and property (including vehicles) of employees at any time whilst they are on the Company's premises or business. It is understood that such checks in themselves do not imply suspicion in relation to the individual concerned.

Whenever practicable an employee will be accompanied by a third party, who is on the premises at the time a search is taking place or at the time that any further questioning takes place.

Employees may be asked to remove the contents of their pockets, bags, vehicles, etc.

Whilst an employee has the right to refuse to be searched, refusal by an employee to agree to being searched can constitute a breach of contract, which could result in his or her dismissal.

The Company reserves the right to call in the police at any stage.

Secondary Employment

Employees must devote the whole of their time, attention and abilities during their hours of work to their duties for the Company.

Prior to undertaking any other employment outside normal working hours, an employee should consult his or her immediate Director. The employee must ensure that it does not interfere or conflict with his or her attendance and duties with Blundells Hill Golf Club Limited.

This does not however, prohibit employees from holding shares in quoted securities for investment purposes only.

The right is reserved to decline requests to carry out secondary employment, and to insist that any secondary employment already being undertaken is stopped. Under no circumstances are employees permitted to use any of the Company's tools, equipment or property (including vehicles) for the purposes of carrying out

secondary employment. Any breach of this Company rule will lead to disciplinary action, which may result in the employee's dismissal.

Short-time Working and Layoff

In the event of a shortage of work for whatever reason, the Company may find it necessary to introduce an arrangement of short time working or a temporary suspension from work without normal pay. In either case this will be done within the provisions of current employment law.

Socialising with Customers or Clients

Employees must not socialise or take holidays with suppliers, external consultants, customers or clients unless the event is authorised by the Company. Should an employee find himself or herself in an unplanned social meeting with a supplier, external consultant, customer or client, the employee should be sensitive to the occasion, exchange pleasantries and then politely distance himself or herself from the situation. If it proves impossible, the employee should safeguard himself or herself by disclosing details of the incident or social event to a Director via line management.

Persistent or blatant flouting of the guidelines will lead to disciplinary action, which may result in dismissal on the grounds of gross misconduct.

Standards of Dress and Appearance

Employees are required to present a professional image at all times when at work and are expected to dress suitably for the needs of the business and the working environment. Employees of Blundells Hill Golf Club Limited represent the Company, and their appearance and grooming are vitally important to give a good impression of the Company to all members, clients and visitors.

Each employee is responsible for his or her standard of personal hygiene. Employees should be aware that their jobs will sometimes mean they get hot and sticky. Every precaution should be taken to eliminate offensive body odours.

During working hours visible body piercing (other than earrings of a moderate size and appearance), tattoos or facial adornments will only be permitted at the discretion of management.

Any protective clothing or safety equipment issued must be properly worn or used.

For food preparation it is important that the food safety regulations are observed and the following rules apply at all times:

- When working in food preparation, the clean protective clothing provided must always be worn.
- Kitchen staff must wear the safety footwear provided at all times when at work.

- Any minor lesions (or cuts) must be covered with a waterproof dressing coloured blue.
- Jewellery, except a plain wedding ring, must not be worn while handling food.
- Smoking is strictly forbidden in a food preparation room or whilst handling food.
- Nose rings are not allowed to be worn by food handlers due to the risk of cross contamination, i.e. bacteria from the nose to food.
- Hair should be tied back and the issued head wear worn by kitchen staff.
- Employees are not permitted to use strong perfume or aftershave.
- If an employee wishes to wear make-up, this must be kept to a minimum.
- Employees must wash your hands frequently with soap (or detergent) in hot running water, using a nail brush as necessary. Disposable paper towels or a hot air hand dryer must be used for drying hands. Nails should be kept short and clean at all times and the wearing of nail varnish is not permitted.
- Employees must always wash their hands:
    - After using the toilet.
    - On entering the kitchens before handling food.
    - Before and after cleaning.
    - After touching the ears, nose, mouth and hair.
    - Between handling raw and cooked foods.

It is the duty of every employee to observe all requirements relating to food hygiene and safety. Any employee found not to be complying with those requirements may render themselves liable to serious disciplinary action and/or prosecution for an offence relating to personal hygiene.

Statements to the Media

Any statements to reporters from newspapers, radio, television, etc. will be given only by a Director.

Territorial Army Leave

Employees who are members of the Territorial Army or similar Reserve Forces are entitled to 2 weeks additional leave each year to attend annual training camp. Confirmation of the dates of attendance and a certificate of attendance should be sent to a Director. Service pay will be deducted from the employee's salary.

Theft / Dishonesty

Where this is alleged the person will be suspended with pay pending the outcome of investigations. Should an employee be given a criminal conviction arising from an act outside the Company's premises which may reflect on the reputation of the Company then instant dismissal will follow.

Trade Unions and Collective Agreements

Blundells Hill Golf Club Limited does not have agreements with any Trade Unions and therefore does not recognise any Trade Unions for negotiation or representation purposes.

All employees have the right to choose to belong, or not to belong, to a Trade Union of their own choice.

Training Courses

Where appropriate, employees will be permitted to attend training courses that are recognised by the Company, usually on a day release basis. The cost of such training courses together with associated training support costs will be met by the Company.

Should the employee leave the Company during the 12 months after completion of the training, a percentage of the training costs is to be reimbursed to the Company. The amount due will be calculated on a pro rata basis depending on the length of service after completion of the training, as follows:

Termination effective from	% of costs repayable
Up to 3 months after the commencement date	100%
3 to 6 months after the commencement date	75%
6 to 9 months after the commencement date	50%
9 to 12 months after the commencement date	25%
More than 12 months after the commencement date	0%

However, if the employee leaves employment before the end of the course, the full amount incurred by the Company for the cost of training will be repayable.

On termination of employment the Company has the right to deduct any outstanding amount due from the employee's final pay. If the provision of pay is not sufficient to meet the sum involved the Company will invoice the employee for the amount due and it is his or her responsibility to meet this cost. The employee agree to this deduction by signing this contract.

Variations to Terms and Conditions

The Company reserves the right in appropriate circumstances to change the terms and conditions of employment. Any such variations will be notified to employees either by way of a general notice or as individual personal notices, whichever is appropriate. Any changes will be made by way of negotiation and appropriate consultation, and the advance notice given by the Company will be

dependent upon length of service and within legislative guidelines.

Workplace Monitoring

In the interests of security and safety, employees are advised that the Company premises, both outside and inside the building, are surveyed by CCTV cameras 24 hours per day. Recordings will be viewed routinely during working hours and where it is found that an employee is in breach of any Company rule the recording may be used in support of disciplinary action.

33 POLICY REVIEW

The Company will review from time to time the operation and effectiveness of all policies and they will be kept under review and their performance monitored.

AUTHORITY TO MAKE DEDUCTIONS FROM WAGES

I accept and agree that the following are express written terms, as contained within my Contract of Employment, which I have read and understood.

The following set down the circumstances, wherein my employer is authorised to make deductions from my wages, including final wages.

****

ANNUAL HOLIDAYS

In the event of your employment terminating during the holiday year and you have taken holidays in excess of the number of days accrued and due to you, at the effective date of termination of your employment, we reserve the right to recover a sum equal to the amount of excess holidays taken by making a deduction from your final pay. You will be notified of such at the time, in writing.

STOCK/PROPERTY

If, following investigation, it is found that as a result of your carelessness, negligence, or failure to comply with our procedures, or by wilful act, we suffer loss, or damage, of cash, stock, fixtures and fittings, or property, (including vehicles), this will be construed as a serious breach of the rules, which could result in your summary dismissal on the grounds of gross misconduct.

We reserve the right to take disciplinary action, and in addition you may be liable to pay the full, or part, cost of making good any losses in respect of cash, stock, fixtures and fittings, insurance excess payments or insurance premium increases sustained by the Company as a result of the loss of, damage to or unauthorised use of any Company property (including vehicles), or that of any client, customer or supplier, which is caused through your carelessness, negligence, recklessness, wilful default or dishonesty.

N.B. This would include losses incurred by us in respect of any hire equipment or costs which we have had to reimburse to a third party.

LEAVING WITHOUT WORKING NOTICE

If, on leaving our employment, you fail to work your full contractual notice, without our prior agreement, an amount equal to any loss suffered by us, or the additional cost of covering your duties for the period not worked, will be deducted from any final monies due to you.

FINES

If you incur any fines for parking or other motoring offences whilst driving one of our vehicles, you will be personally accountable for the payment of such fines. Fixed penalty notices are normally reported directly to us by the authorities. We reserve the right to pay such fixed penalties on your behalf and deduct the cost from your wages or salary.

OTHER DEDUCTIONS

If, either during or on the termination of your employment, you owe the Company money as a result of any loan, overpayment, default on your part or any other reason whatsoever, the Company shall be entitled to deduct the amount of your indebtedness to it from any payment or final payment of wages which it may be due to make to you and you expressly consent to any such deductions pursuant to Part II of the Employment Rights Act 1996. Such deductions may include, but are not limited to:

- an overpayment of, or advancement on, wages, bonus, commission or expenses, whether made by mistake or otherwise
- any loans
- the market value of any unreturned Company property on the termination of employment
- the repayment of any contractual or discretionary sick pay where the reporting requirements have not been followed or the absence is unauthorised
- the repayment of any contractual or discretionary sick pay where monies are also received for the period of sickness absence under an insurance policy
- the payment of any sum received from the court as loss of earnings for undertaking jury service where your wages have been paid by the Company during your absence

- attachment of earnings orders, child support maintenance, judgment debts, payments under an administration order, sums ordered to be paid following a criminal conviction, student loans or any other payment required by law.

If, on the termination of your employment, your final payment of wages is not sufficient to meet your debt due to the Company, you agree that you will repay the outstanding balance to the Company within one calendar month of the date of termination of your employment, such payment to be made as agreed with the Company

*** * * * * * * * * * * * * * * * * ***

I further understand that on any occasion when my employer intends to implement one or more of the above conditions, I will receive written notification of that fact and a statement of the amount to be deducted.

I hereby give my written consent for my employer to make deductions, in the circumstances described above.

Name: ..... Department: .....

Signature: ..... Date: .....

Witnessed on behalf of the Company: .....