DATA PROTECTION AND RECORD RETENTION POLICY

The Company collects, stores and processes personal data in respect of its employees, suppliers, contractors, customers and others with whom it communicates. In the course of your employment you may come into contact with or need to use confidential information about other individuals and you must comply with the terms of the **Data Protection Act 1988 (the Act).** Individuals protected under the Act are known as 'data subjects'.

The Act sets out the legal principles relating to the handling of personal data stored on computer or in manual records. This policy sets out the principles of the Act. If you are in any doubt about what information you can or cannot disclose and to whom, do not disclose any personal information until you have sought further advice from your line manager or the Legal Department. You can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A breach of the Act by you will be dealt with under the Company's disciplinary procedures. If you access another's personal record without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal. By signing your contract of employment you have expressly consented to the Company holding limited and appropriate sensitive personal data about you.

The Data Protection principles

There are eight data protection principles under the Act and the Company and all its employees must comply with these principles at all times.

1. Used fairly and lawfully.

This means data must not be processed unless the individual has given its consent or the use is specifically authorised in the Act. Sensitive personal data may only be processed with the explicit consent of the individual and consists of information relating to:

- race or ethnic origin
- political opinions and trade union membership
- religious or other beliefs
- physical or mental health or condition
- sexual orientation
- Criminal offences, both committed and alleged.

2. Used for limited specifically stated purposes

The data can only be collected for a specific purpose for which the individual was made aware. Any change in the purpose must be first notified to the individual prior to any use or retention of the data.

3. Adequate, relevant and not excessive

The Company will only obtain and retain personal data if there is a clear reason for collecting and retaining the data.

4. Accurate and kept up-to-date

The Company will review files held of a personal nature to ensure they do not contain a backlog of out-of-date information. The information held should be up to date and must be refreshed and updated regularly. In relation to you your personal information you must inform the People Department of any changes as soon as practicable so that the records can be updated. The Company cannot be held responsible for any out of date information if you have not notified the relevant change.

5. Kept for no longer than is necessary

The Company will keep personnel files for no longer than six years after termination of employment. Data relating to unsuccessful job applicants will not be retained for more than six months. Other categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a period of time will be destroyed after six months.

6. Used according to the Act

This means that an individual may:

(a) Request access to any data held about them by the Company.
(b) Prevent the processing of their data for direct marketing purposes.
(c) Request to have inaccurate data amended or deleted.
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. Data to be securely stored

Records containing personal data must be stored securely to avoid potential misuse or loss. Manual records should be stored in a lockable secure cabinet with keys issued on a limited and strictly necessary basis. Electronic data must be password protected and passwords regularly changed. . Data stored internally or externally by the Company will not be transferred outside the European Economic Area. The Company will ensure that any third party data storage provider will be vetted to ensure that it has demonstrated compliance with the requirements of the Act.

- Data and records which are active should be stored in the most appropriate place for their purpose.

- Data should not be held or copied onto external or individual storage devices or hard drives but must only be stored on the Company secure systems which can be accessed by users remotely when connected to the internet.

- Data and records which are no longer active, due to their age or subject, should be archived and securely stored off site or disposed of appropriately to ensure that copyrights are not breached and to prevent personal data falling into the hands of unauthorised personnel. Refer to the Company's archiving procedure for further information.

8. Transfer to another country

Personal data will not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

Right to access personal information

An individual has the right on request, to receive a copy of the personal information held by the Company including your personnel file, and to request that any inaccurate data be corrected or removed. You have the right:

- To be told by the Company what information they hold and for what purpose your personal data is being processed.
- To be given a description of the data held and the recipients to whom it may be disclosed.
- To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data.
- To be informed of the logic involved in computerised decision-making.

Upon written request, the Company will provide a statement regarding the personal data held about you.

Complaints that the rules set out in the Act are not being followed should be raised with the Legal Department. If the matter is not resolved satisfactorily it should be escalated to the Director of Legal, Risk and Compliance.

Employees have some rights to prevent data being processed where such processing is likely to cause you or another person unwarranted or substantial damage or distress and you can prevent processing of data for direct marketing purposes even where consent has been previously given.

Your obligations in relation to personal information

You should ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly, before releasing personal information by telephone.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the People Department responsible for dealing with such requests.

DATA PROTECTION AND RECORD RETENTION POLICY

Retention Statement

The Company policy in relation to data retention is that personal data "shall not be kept for longer than is necessary for that purpose".

The Company will retain data and records as required per the guidance periods shown in Appendix A. Reasons for retention will include the following:

- Statute requires retention for a set period (see Appendix A)
- The record contains information relevant to legal action which has been started or is in contemplation
- Records and information should not be amended or disposed of until the threat of litigation has been removed
- The records are maintained for the purpose of retrospective comparison
- HR and employee records retained for the purposes of managing civil claims.

Destruction and disposal procedures

The Company will ensure that all data is disposed of properly and all information of a confidential or sensitive nature on paper, card, microfiche, or electronic media will be securely destroyed when it is no longer required.

- A record of externally archived documentation must be maintained.
- Any confidential or sensitive paper data should be disposed of by shredding
- All other paper can be disposed of in the boxes or bins provided in offices for environmentally-friendly disposal of non-confidential and non-sensitive paper waste.
- Media being destroyed because of damage or because obsolete should be physically destroyed by being cut into pieces or other ways prior to disposal
- Where disks, tapes, DVD or CD ROM are being used to supply data to third parties they should, at the very least, be reformatted before the files are saved on to it.
- Ensure destruction of back-up copies of any data.

COMPLIANCE WITH THE ACT IS YOUR RESPONSIBILITY. IF YOU HAVE ANY QUESTIONS OR CONCERNS ABOUT THE INTERPRETATION OF THESE RULES, CONTACT THE HUMAN RESOURCES DEPARTMENT.

Appendix A
Document Retention Guidelines
Part 1 Summary of main legislation regulating the statutory retention periods

Document	Recommended retention period	Justification
Accident books, accident records Visitor records	Three years after date of last entry	Reporting of Injuries Diseases and Dangerous Occurrence Regulations 1995 (RIDDOR) (SI 1995/3163) as amended. Special rules relating to hazardous substances. Social Security (Claims and payments) Regulations 1979
Accounting documents • Payroll (non HMRC returns) • Statutory accounts • Bank statements • Cheque books • Expense claims • BACS payments	Six years from creation	Section 221 Companies Act 1985 as modified by the Companies Act 1989 and 2006.
Contract documentation, to include: • Construction contract • Subcontractor orders • Purchase orders • Professional appointments • Contract correspondence • Minutes • Telephone conversation notes	12 years from practical completion for those contracts executed as a deed and 6 years for contracts executed under hand	The law permits claims for negligence to be brought within three years of the claimant having the knowledge required to bring an action for damages and the right to bring such action subject to an overriding limit of 15 years
Income tax and NI returns , income tax	Not less than 3 years after the end of the	The Income Tax (Employments)

returns and correspondence with the Inland Revenue	financial year to which they relate	Regulations 1993 (SI1993/744) as amended
HR records • Personnel files • Training records • Redundancy records and calculations of payments, refunds, notification to the secretary of state • Time cards • Medical records • Statutory maternity pay	Indefinitely for historical purposes and to assist with an a civil action claim	Limitation Act 1980 Control of Asbestos at Work Regulations 1987 The Working Time Regulations 1998 (SI1998/1833)
• National Minimum Wage records	Three years after the end of the pay reference following the one that the records cover	National Minimum Wage Act 1998
• PAYE documentations including CIS	Current year plus three prior years	HMRC – Keeping records for business – what you need to know
• Retirement Benefit Schemes records of notifiable events e.g. incapacity	Six years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI1995/3103)
• Statutory Maternity Pay records, calculations,	Three years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960) as amended.
• Statutory Sick Pay records, calculations,	Three years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI1982/894) as amended.
• Wage/ salary records (bonuses/ overtime/expenses).	Six years	Taxes Management Act 1970
• Parental leave	Five years from birth/adoption of child or	

	18 years if the child receives a disability allowance	
VAT documentation • Purchase invoices • Contract sales invoices • Sundry sales invoices	6 years from creation.	HMRC guidance is to retain for six years

Part 2 Recommended retention periods (where no statutory retention periods exist)

Actuarial Valuation Reports	Permanently	
Application forms and Interview notes for unsuccessful candidates	12 months	
Assessments under Health and Safety Regulations	Permanently	
Deed books	Indefinitely	Company History and family
Insurance Certificates	Permanently	
Inland Revenue approvals	Permanently	
Money Purchase details	Six years after transfer or value taken	
Pension scheme investment policies	Twelve years from the ending of any benefit under the policy	
Pensioners records	Twelve years after benefit ceases	
Statutory Books	Indefinitely	
Trade Union agreements	10 years after ceasing to be effective	
Trust deeds and rules and trustees minute book	Permanently	