GET Solutions
Data Protection Policy

1. Introduction

This document sets out the obligations of ("the Company") with regard to data protection and the rights of people with whom it works in respect of their personal data under the Data Protection Act 1998 ("the Act").

This Policy shall set out procedures which are to be followed when dealing with personal data with respect to employees and third parties such as customers. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties and its employees. The Company shall ensure that it handles all personal data correctly and lawfully.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

2.1 Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met);

2.2 Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;

2.3 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;

2.4 Must be accurate and, where appropriate, kept up-to-date;

2.5 Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;

2.6 Must be processed in accordance with the rights of data subjects under the Act;

2.7 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

2.8 Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Rights of Data Subjects

Under the Act, data subjects have the following rights:

- The right to be informed that their personal data is being processed;
- The right to access any of their personal data held by the Company within 40 days of making a request;
- The right to prevent the processing of their personal data in limited circumstances; and
- The right to rectify, block, erase or destroy incorrect personal data.

4. Personal Data

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company only holds personal data which is directly relevant to its employees and customers. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Company:

- Identification information relating to employees and customers including, but not limited to, names and contact details;
- Equal opportunities monitoring information including age, gender, race, nationality and religion;
- Health records including details of sick leave, medical conditions, disabilities and prescribed medication;
- Employment records including, but not limited to, interview notes, curricula vitae, application forms, assessments, performance reviews and similar documents;
- Details of salaries including increases, bonuses, commission, overtime, benefits and expenses;
- Records of disciplinary matters including reports and warnings, both formal and

informal;

- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes;
- Records of customers' bank details

5. Health Records

The Company holds health records on all employees which are used to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records will include details of sick leave, medical conditions, disabilities and prescribed medication. Data under this heading will be used by management only and will not be revealed to fellow employees and peers (unless those employees are responsible for health records in the normal course of their duties).

Employees have the right to request that the Company does not keep health records on them. All such requests must be made in writing and addressed to Lisa Bainbridge, Operations Manager.

6. Benefits

In cases where employees are enrolled in benefit schemes which are provided by the Company (including, but not limited to, pensions and healthcare) it may be necessary from time to time for third party organisations to collect personal data from relevant employees.

Prior to collection, employees will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.

The Company shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

7. Trade Unions

The Company will provide the following personal data concerning relevant employees to bona fide trade unions where those unions are recognised by the Company. The following data will be supplied:

- Name;
- Job Description;
- Any relevant data as agreed with the employee dependent on the circumstances

All employees have the right to request that their personal data is not supplied to trade unions under this Section.

8. Monitoring

The Company may from time to time monitor the activities of employees. Such monitoring

may include, but will not necessarily be limited to, internet and email monitoring. Any employee that is to be monitored shall be informed in advance of such monitoring.

Under no circumstances will monitoring interfere with an employee's normal duties.

The Company shall use its best and reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities and under no circumstances will monitoring take place outside of the employee's normal place of work or work hours.

9. Processing Personal Data

Any and all employees' and customers' personal data collected by the Company is collected in order to ensure that the Company can efficiently manage its employees and customers and conform with its equal opportunities obligations. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data in view of the purpose(s) for which it was collected and is being processed.

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully;
- Employees are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and
- All employees can exercise their rights set out above in Section 3 and more fully in the Act.

10. Data Protection Procedures

The Company shall ensure that all of its employees, contractors, agents, consultants,

partners or other parties working on behalf of the Company comply with the following when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data may be transmitted over secure networks only – transmission over unsecure networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted;
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

11. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Designated Officer") within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are made fully aware of both their individual rights and responsibilities and the Company's responsibilities under the Act and shall be furnished with a copy of this Policy.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly

evaluated and reviewed.

- All personal data shall be kept up-to-date. If an employee's personal data changes the employee shall be under a duty to inform the Operations Manager of those changes.
- Any personal data which is out-of-date or no longer required shall be deleted or otherwise destroyed.
- The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Act.
- Where any contractor, agent, consultant, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

12. Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to see the information which the Company holds about them.

- SARs must be made in writing, accompanied by the correct fee.
- The Company currently requires a fee of £10 (the statutory maximum) with all SARs.

Upon receipt of a SAR and fee the Company shall have a maximum period of 40 calendar days within which to respond. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

13. Employee Records and Retention

The Company shall retain all employee and customer records following the end of employment for the following periods:

Refer to Appendix 1

14. Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

15. Implementation of Policy

This Policy shall be deemed effective as of. 1 August 2013. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved & authorised by:

Name: Lisa Bainbridge

Position: Operations Manager

Date: 1 August 2013

APPENDIX 1

Record Retention Guide

Document	Retention	Period Reason
Insurance		
Policies	12 years after lapse	Legal
Claims	3 years after settlement	Commercial
Schedules/Disclosures	12 years	Legal
Accident Record Book	Permanent	Legal
Public & Product Liability Policies	Permanent	Legal
Cash Records		
Bank Paying- In Counterfoils	6 years	Legal /Tax
Cheque/Remittance Advices	6years	Legal
Bank/GIRO Account Statements	6years	Legal
Daily Cash Book	6 years	Legal
Banking Returns	6 years	Legal
Unpresented Cheque Lists	6 years	Legal
Bank Reconciliations	6 years	Legal
Employees pay receipts	6 years	Legal
Petty Cash Records	6 years	Legal
Main Cash Book	Permanent	Legal
Cash/Cheques Received Sheets	Current plus 6 years	Legal
Petty Cash Returns	6 years	Commercial
Title Deeds etc.		
Title Deeds and Property Documents	12 years after ceased	Legal
Contracts/Agreements		
Under Seal	12 years after expiry	Legal
Others	6 years after expiry	Legal
Royalty	1 year after expiry	Legal

Payments/Agreements		

Record Retention Guide

Document	Retention Period	Reason
Stores Documents		
Goods Received Register	4 years	Audit
Inward Invoice register	6 years	Legal
Stock Control Records	7 years	Legal
Transport Records		
Drivers Log Books	1 year	Commercial
Other records	2 years after vehicle disposal	Commercial
Tachographs	3 years	Legal
Property Receipts		
Leases	12 years from lease end	Legal
Architect/Builder agreements	6 years from contract end	Legal
Planning Permission	12 years form interest end	Legal
Management Information		
Accounts	6 years	Commercial
Others	6 years	commercial
Trade Mark Papers		
All related documents	Permanent	Commercial
Expired Patents	12 years	Legal
CE marking details	10 years from cessation of manufacture	Legal
Quality Records		
Internal & External Audits	6 years	Review
Old Procedures and Revisions	6 years	Review
Management Reviews	6 years	Audit
Defects and correct action Records	6years	Review
Calibration Records	6 years	Commercial
Others	6 years	Commercial

Documents	Retention Period	Reason
Employee Records		
Unsuccessful Job Applications	1 year	Commercial
Medical Records	30 after expiry	Legal
Accident Reports	Working life Employee	Legal

Pension Details	10 years after and of benefits	Legal
Payment Changes	6 years	Legal/Tax
Payroll Control	Current plus 6 years	Legal/Tax
Amended Code Number Notice	6 years	Legal
Trust Records	Permanent	Legal
Group Health/Personal Accident	12 years after benefit ends	Legal
Staff personal Records	7 years after Termination	Legal
Company Executive Records	12 years	Legal
Salary Register	6 years	Legal
Expense Accounts	7 years	Legal/Tax
Industrial Training	6 years	Commercial

Wages

P45,P58,P6,P60	6 years	Legal/Tax
Income Tax Pat Details	6 years	Legal/Tax
Pension Contributions	Permanent	Commercial
National Insurance Contributions	12 years	Commercial
Schedule of Deductions	6 years	Audit
Clock Cards	2 years	Audit
Pay Advice	Current plus 1 year	Legal
Payroll	Current plus 6 year	Legal
Annual Earnings Summary	Current plus 12 years	Legal

Sub- Contractors Documents

SC60 etc.	6 years	Legal/Tax
Other Tax	6 years	Legal/Tax
National Insurance	6 years	Legal/Tax
Timesheets etc.	3 years	Legal

Documents	**Retention Period**	**Reason**

Suppliers Accounts

Cheques/Remittance Advice	6 years	Legal
Cash Book	10 years	Legal
Cost Control Ledger Analysis	6 years	Legal
Invoices Revenue	6 years	Legal
Invoices Capital	12 years	Commercial
Purchase orders Revenue	4 years	Audit

Purchase orders Capital	3 years after expiry	Audit
Quotations Capital	12 years	Audit
Quotations Revenue	7 years	Audit
Customs and Excise Returns	6 years	Legal
VAT Deferments	6 years	Legal

Assets

Ledger Sheet	12 years	Legal
Consolidated Accounts	12 years	Commercial
Disposal of Assets	12 years	Commercial
Annual Depreciation	3 years	Audit

Sales Records

Customer Complaints	7 years	Legal
Customer Orders	6/12 years after expiry	Commercial
Customer Enquiries	1 year if unsuccessful	Commercial
Sales/Journal Entries	12 years	Legal/Tax
Nominal and Private Ledgers	Permanent	Legal/Tax
Journal Vouchers	3/6 years	Legal/Tax
Sales Invoices/Credit Notes	6 years	Legal
Consignment Notes	6 years	Legal
Outstanding Notes Schedule	6 years	Legal
Statements	2 years	Audit
Overdue Account Letters	Until Paid	Commercial
Project Files	6 years	Legal

Which documents should be securely destroyed?

Depending on your particular are of business these documents will vary slightly as some information may be limited to your industry. However there are many common documents that hold sensitive information that should be kept in a secure manner and also destroyed in a secure manner at the end of its life.

To give you an idea of information that must be kept confidential and therefore must be stored or destroyed in a secure manner we have complied the following list:

HR FILES:

Application forma & CVs
Interview Notes
Employee contracts
Copies of passports or driving Licence
Name, address, DOB, NI number forms
Contact details
Medical details
Bank account details

Administration:

Correspondence
Junk Email
Reports
Schedules
Training Records
Manuals
Order information
Meeting Minutes

Ethnic background forms
Criminal records Bureau forms

Account Details:
Payroll details
Bank account details including statements
Client details
Budgets
Invoices & receipts
Financial reports
Supplier information including invoices
Contracts
Purchase orders
Accounts payable/receivable
Ex-employee tax records

Job & workload sheets
Customer service files
Inventory lists
Memos

Research:
Plans, designs & blueprints
Lab books
Development process papers
Specifications
Reports
Competitive test sheets
new product test

Sales and Marketing Files:

(Prospective) Client details
Quotes and tenders
(Prospective) Customer Correspondence
Out of date brochures or leaflets
Out if date business cards
Old letterhead paper & compliments slips
Targets & business projections

Other materials:
CD & DVS
Video or data tapes
ID tags & cards
X-rays
Microfilm rolls
Microfiche & jackets