

Data Protection Policy

Hall Court-Policy-001
Revision 1.0

06.08.2018



Author
M Harrison

Process owner
S Peat

Issued by:	S Peat	Date	06.08.2018
Approval Document	S Peat		
Review due:	Annually	Date	



Document Tracking and History

A Document Distribution

Copy No.		Location
1	:	Document Repository (word) (electronic)
2	:	Issued Document Repository (pdf)

B Revision History

Rev. #	Procedural change #	Changed by	Date	Brief description of change
1.0				New issue

C Authorised personnel

Authorised personnel are current employees at the time of issue.



Table of Contents

Document Tracking and History	2
A Document Distribution	2
B Revision History	2
C Authorised personnel	2
Table of Contents	3
1. Purpose	4
2. Responsibilities	4
3. Related Documentation	4
4. Procedure	4
5. Data Protection Officer	6

1. Purpose

This policy describes the company rules regarding collecting and storing personal and sensitive data.

2. Responsibilities

All employees are expressly required to read, understand and abide by the rules and guidelines as outlined in this document. Employees will be advised of any changes to this policy from time to time and are required to familiarise themselves with any changes.

3. Related Documentation

Data Protection Act 2018
General Data Protection Regulations 2018

4. Procedure

The company holds and processes information about its employees and other individuals for various purposes, for example in connection with Employment details, Health & Safety, Client contacts details, Information technology.

All staff share the company's responsibilities under the Data Protection Act 2018 (inc1998 act) and General Data Protection Regulations 2018 to ensure that data from living individuals can be identified (personal data) is processed fairly, stored responsibly and securely and in accordance with the law, whether this relates to employees, clients or collaborators.

The company is committed to complying with the data protection principles which are set out in the 2018 act and which serve to protect the individual's right to privacy. In summary the company will strive to ensure that personal data is;

- Processed fairly and lawfully
- Obtained by consent for specified and lawful purposes
- Adequate, relevant and not excessive for those purposes
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in accordance with an individual's rights under the act
- Protected by appropriate measures against unauthorised and unlawful processing, accidental loss or destruction.
- Not transferred to a country outside the European Economic Area, unless with consent and that country has equivalent levels of protection for personal data

The company will process personal data about you in accordance with and to the extent permitted by the Data Protection Act 2018. This is in order for the company to carry out its legitimate business interests, for example paying salaries and contacting clients. Your personal data may be kept securely electronically or hard copy format.

Your personal data may be disclosed or transferred to;

- Other employees of the company
- Other persons or collaborator's as may be reasonably necessary for the purposes of or in connection with your employment, clients requirements
- As otherwise required or permitted by law

You agree that the company may, from time to time post personal data about you on it's website for it's legitimate business purposes. For example, the company may promote particular departmental activities on the website and include the name and work contact details of some individuals in that department. You should be aware that the website is, in theory accessible worldwide.

Sensitive personal data is information as to a data subject's racial or ethical origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health conditions, sexual life, offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed by the data subject , including the outcome of those proceedings.

You agree that the company may process sensitive personal data relating to you, in connection with your employment or the activities of the company. The company envisages at this time the need to process sensitive personal data for the following purposes;

- Data relating to the ethnic origin of employees or the company may be processed for the purposes of equal opportunities monitoring
- Medical, Occupational Health records need to be processed for administering sick pay, the provision of healthcare, general welfare and monitoring attendance and capability
- In exceptional circumstances, the company may need to information regarding criminal convictions or alleged offences in connection, for example with any disciplinary proceedings or other legal obligations

You agree that the company may disclose or transfer these categories of sensitive personal data to other persons or collaborators outside the company if it is required or permitted to do so by law.

Processing, in relation to the company's use of information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

- Organisation, adaption or alteration of the individuals information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data; or
- Destruction of the information or data
- We will store data for 7 years

The company's data protection officer is Stephanie Peat, Stephanie has overall responsibility for data protection. If you have any queries concerning this policy or any data protection issues you should contact the data protection officer directly.

It is important that all employees ensure that;

- Any personal data which they have access to or hold is kept securely and in line with this policy
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party

You must not, under any circumstances, disclose any personal information or data concerning another employees or client or any other individual over the telephone for example, personal information such as; Home address and Telephone numbers.

In the case of an apparent emergency, any unusual request for personal information should be directed to the data protection officer immediately.

All personal data must be kept securely and examples of how this may be done include;

- Keeping all personal data locked in a filing cabinet with restricted access and authorisation
- If the data is held electronically, ensuring that it is password protected or kept only in protected folders which itself is secure
- Emailed only by secure means

Unauthorised disclosure of personal information can have very serious consequences for the company and it's employees. It may be found to be a disciplinary offence and may constitute gross misconduct leading to summary dismissal.

Obtaining or disclosing personal data or another individual, employee or client without the company's consent may also attract personal criminal liability.

All employees must ensure that any personal data which you provide or collect from a client is both accurate and up to date. Any personal data changes must be provided to the data protection officer as soon as possible.

All employees and any other individuals have a right under the Data Protection Act 2018 to request access to personal data relating to themselves which is held by the company in electronic format and any hard copy format that forms part of our recognised filing system, held in a structured and secure way.

If you wish to see personal data relating to you, you must apply in writing to the data protection officer. The company may charge an administration fee of no less than £10 and will normally respond to a written request within 40 days.

5. Data Protection Officer

Stephanie Peat
1 St Leonards Close
Dinnington
Sheffield, S25 2RL