HUNTSWOOD

DATA PROTECTION POLICY

APPROVAL CONTROL

ROLE	NAME	DATE
Director of Risk	Steve Mills	29/01/2016

VERSION CONTROL

VERSION	AUTHOR NAME	VERSION CHANGES	DATE
1.0	Carol Hawker	Policy written and approved	29/01/2016
1.1	Carol Hawker	Policy reviewed, no changes required	20/02/2017
		-	

TABLE OF CONTENTS

BACKGROUND

The Data Protection Act 1998 (DPA) was introduced to give effect to the European Data Protection Directive. The DPA was passed on 16 July 1998 and came into force 1 March 2000.

The enforcement of the DPA is administered by the Office of the Information Commissioner, an independent officer who reports directly to Parliament. The DPA covers any Personal Data processed in any form (electronic/paper/CCTV etc.).

The DPA gives individuals certain rights concerning information held about them by Huntswood, and requires Huntswood to be open about the use of such data and ensure personal data is processed in a responsible and secure manner.

The DPA does not cover the processing of personal data in the following circumstances:

- Where the data relates to individuals who are no longer living, or who live outside the UK

- Where the data is stored in a manual system that cannot be readily accessed and updated – for example the response to a market research survey which has not collected the names of individuals

APPLICABILITY

This Policy applies to all Huntswood Representatives acting for, or on behalf of Huntswood.

Any breach of this Policy shall constitute a disciplinary, contractual and possibly a criminal matter for the individual concerned and may cause serious damage to the reputation and good standing of Huntswood.

SCOPE

Typical automated data processing systems

The automated data processing systems covered by the DPA are extensive and continually evolving with developments in technology. Typical systems include:

- Electronic computers, whether mainframe, personal computers, laptop, tablet
- Internet and intranet sites
- Video systems, including CCTV and webcams
- Document imaging systems
- Voice recording systems
- Telephone systems that use caller identification
- Mobile phones
- Microfilm or microfiche
- Relevant filing systems (see below)

Relevant filing system

In addition to automated systems as above, the DPA regulates personal data held on paper in a non-automated relevant filing system. The DPA defines this as 'specific information relating to individuals, where even though the information is not processed automatically in response to programmed instructions, the information is readily accessible by reference to that individual, or by reference to criteria relating to individuals'. In simple terms this means a manual filing system holding personal data that can be readily accessed and updated, for example employee HR files held in a cabinet.

POLICY STATEMENT

Huntswood needs to gather and use certain information about individuals to enable it to conduct its business; information can include employees, customers, suppliers, business contacts and other people the business has a relationship with.

This data protection policy sets out Huntswood's position and ensures Huntswood:

- Complies with data protection law and follows good practice
- Protects the rights of individuals
- Is open about how it processes and stores individuals' data
- Provides training and support for employees who handle personal data
- Protects itself from the risks of a data breach

RESPONSIBILITIES

Huntswood representatives have the following responsibilities in connection with data protection:

- To undertake training on a regular basis as determined by Huntswood
- To apply the regulations using Huntswood procedures, systems and controls to protect the rights and privacy of individuals
- To be aware of potential disciplinary action as a result of not complying with DPA regulations

HR, QA and Resourcing Responsibilities

Huntswood's Human Resources (HR), QA and Resourcing Departments have the following responsibilities in connection with data protection:

- Ensuring that the business complies with the DPA Code of Practice for employees and employers
- Ensuring that induction packs for new starters contain information on Huntswood data protection procedures
- Defining the disciplinary actions for DPA offences, and ensuring the terms and conditions of employment state these disciplinary actions
- Ensuring that all relevant staff are provided with training on data protection at regular intervals (at least every two years), and that training records are kept on each employee

DATA PROTECTION PRINCIPLES

Huntswood is required to comply with the eight data protection principles set out below, with regard to Personal Data processed by or on behalf of the business:

Personal Data shall be:

1. Processed fairly and lawfully (and not processed unless one or more of the specified statutory conditions has been satisfied). Processing of Sensitive Personal Data is subject to additional statutory conditions;
2. obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with such purposes;
3. adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept no longer than necessary for the purpose(s);
6. processed in accordance with Data Subjects' rights (see below);
7. subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data;
8. not transferred to a country or territory outside 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.

NOTIFICATION

Notification (also known as registration) is a mandatory process that Huntswood is required to perform annually to provide the ICO with details of the data held, for whom it is held and the purpose for which it is held. The details are added by the

ICO on the Notification entry into the Data Protection Register. This is available for public inspection online at https://ico.org.uk

EXEMPTIONS FROM THE REGULATIONS

The DPA permits exemptions from the eight data protection principles in specified circumstances. These include national security, crime and taxation, legal proceedings and research and forecasting. Failing to comply with an exemption could be an offence.

CONDITIONS FOR PROCESSING PERSONAL DATA

Collecting Data

All Huntswood Representatives must have regard to the DPA principles and must only process data in accordance with their Departmental Procedures.

Maintaining Accuracy of Data

All Huntswood Representatives must ensure that they follow their departmental procedures for collecting data and for checking the data at regular intervals for accuracy.

REMOVING DATA AFTER EXPIRY OF ITS RETENTION PERIOD

Huntswood has defined the data retention periods for different types of personal data taking into consideration the applicable regulatory requirements in the Control of Records Policy which can be found on the Vault. Electronic data shall be removed from the database and paper data from storage and securely destroyed in accordance with the Secure Disposal and Reuse Policy.

INFORMATION SECURITY ISO27001

Huntswood must ensure that adequate security measures are in place for the data held. Huntswood are ISO27001 accredited and consequently all of the following documents are available for viewing on The Vault:

- Security Policy
- Access Control Policy
- Acceptable Usage Policy
- E-mail Policy
- Classification and Labelling Policy
- Control of Documents
- Control of Records
- Secure Disposal and Reuse Policy

RIGHTS OF THE DATA SUBJECT

Data Subjects whose information is processed by Huntswood have a right to:

- be told if any Personal Data is held

- be told for what purpose the data is processed
- be told to whom the data has been or may be disclosed
- a copy of the data with any unintelligible terms explained
- information about the source of the data
- an explanation as to how automated decisions have been taken
- have any inaccuracies in the data corrected

DATA SUBJECT ACCESS REQUESTS (DSAR)

A Data Subject Access Request allows an individual to request a copy of all information held on them. The Data Controller must respond to this request within 40 days and can impose a charge of up to £10.00. As far as employees of Huntswood are concerned, no charge will be made for copies of information. Before releasing the data, the Data Controller must ensure that those seeking access are who they say they are. Data should not be provided on any other individual other than the individual making the request.

Failure to comply with a DSAR may result in the ICO taking enforcement action against Huntswood, and the individual concerned would be entitled to claim compensation through the courts if damage had been caused as a result of Huntswood not meeting any requirements of the Act.

All DSAR's should be referred to the DPO who will record the date the DSAR was received and monitor to ensure adherence to the due date.

TRANSFER OF DATA

The DPA limits the transfer of personal data to within the European Economic Area (EEA), and to some designated countries outside the EEA which are considered as having adequate data protection policies. Currently Huntswood does not transfer data outside the EEA.

EXCEPTIONS

An exception to the requirement not to disclose personal data other than in accordance with the rights of subject access is where information is requested by a Government Department, Local Authority or any other Authority administering housing benefit or council tax benefit. Examples would be Customs & Excise, the Police and the Benefits Agency. These bodies are entitled to information for the purpose of prevention and detection of crime. It is an offence not to provide this information if requested.

All enquiries from such organisations should be referred to the DPO promptly.

EMPLOYEE DATA RECORDS

Human Resources hold information about every individual employed by Huntswood. The holding of this information is subject to the DPA.

The purposes for processing employee Personal Data are as follows:

- administration and payment of salary and other benefits
- performance appraisals and training
- career planning and management forecasts
- negotiations and communications
- recording of working time and statutory records where necessary

The information that is held by HR is factual information and is not used for any other purpose than that related to employment issues. This information shall not be passed on to another company or used for the purpose of marketing without the prior consent from the individual concerned.

There may be other circumstances in which employee Personal Data will be disclosed to third parties. Usually consent will be obtained first, but that will not always be appropriate. For example, if a Huntswood Representative should enter into a dispute with Huntswood, Huntswood reserve the right to disclose all relevant personal details about you to our legal or other professional advisers in order to protect our position.

Every Huntswood employee has the right to see the information held on them by HR at any time. Please see the section of this Policy on Data Subject Access Requests for further details.

Types of Data Held

The following is a list of information held by HR :

- Full Name
- Address
- Contact Telephone Numbers
- Date of Birth
- Nationality
- Next of Kin Contact Details
- National Insurance Number
- Payroll Details
- Original Job Application Form/CV and Copy Passport/Driving Licence for Identification/Right to work in the UK
- Copies of Appraisals
- Training Details
- Salary Increases
- Bonus Awards
- Travel Loans
- Annual Leave and Sickness Records
- Disciplinary Details
- Grievance Details

For details of how long information is held on employees, please refer to the Control of Records Policy.

CCTV - CRIME PREVENTION AND/OR STAFF MONITORING

Huntswood uses CCTV for maintaining the security of property and premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about Huntswood Representatives , customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the Data Subjects themselves, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

ENFORCEMENT

Should a Huntswood Representative appear to have contravened any of the data protection principles in such a way so as to result in the possibility of a complaint being made, or compensation being sought against Huntswood, Huntswood reserve the right to take appropriate disciplinary action. Contravention would mean, but not limited to:

- any deliberate contravention of one or more of the data protection principles which results in a potential claim for damages against Huntswood;
- disclosing Personal Data relating to anyone who is a Data Subject of Huntswood to a third party without that Data Subject's express or implied consent;
- selling (or attempting to sell) Personal Data relating to a Data Subject of Huntswood.

Huntswood also reserves the right to take such other action short of dismissal, including removing the right of access to Personal Data, as may be appropriate in the circumstances.

COMPLAINTS

Huntswood will respond to any information rights concerns received, clarifying how the individual's personal information was processed in that case and where an error has occurred it will explain how it will put right anything that's gone wrong.

If a member of the public has engaged with Huntswood but is still dissatisfied with the outcome, they may report their concern to the ICO.

If an employee believes that another employee may have infringed their data protection rights a complaint may be made in accordance with Huntswood's Grievance Procedure.

All complaints should be referred to the DPO who will record the date the complaint was received and monitor the response to ensure completeness.

TABLE OF DEFINITIONS

The table of definitions provides definitions of terms used within the policy document

TERM	DEFINITION
Huntswood Representative	Anyone who works for or on behalf of Huntswood.
Personal Data	Data relating to a living individual who can be identified from that data or from other information in the possession of the Data Controller. This information can be as little as a name, address or e mail address.
Sensitive Personal Data	Personal data, which includes one or more of the following: Racial or ethnic origin, political opinion, religious belief, physical or mental health, membership of a trade union, sexual orientation, criminal convictions, proceedings or settlements.
Processing	Any operation involving personal data including obtaining, recording, collecting, use, retrieval, consultation, disclosure, adaption, alteration, combination, destruction and erasure.
Data Processor	A person or organisation, other than an employee of the Data Controller, that

	processes personal data on behalf of the Data Controller.
Data Controller	A person or organisation that determines the purpose and manner in which personal data is to be processed.
Data Subject	An individual who is the subject of personal data.
Data User	Any employees whose work involves processing personal data.
Data Protection Officer (DPO)	The person with responsibility for ensuring compliance in all matters involving the DPA.

POLICY RESPONSIBILITIES

The following table defines the business roles and their responsibilities in regard of the policy document.

RESPONSIBILITY	ROLE	DEFINITION
Owner	Director of Risk	The Owner ensures the policy is reviewed and maintained on a regular basis
Reviewer	Risk & Audit Manager and Data Protection Officer	The Reviewer ensures the policy document aligns with relevant legislation and company requirements
Author	Risk & Audit Manager and Data Protection Officer	Shall update the policy document in a succinct time frame on receiving updates from the reviewer and in accordance with company policy writing guidelines
Policy Audience	All Huntswood Representatives	Must apply the business policy to the business they undertake on behalf of Huntswood

APPLICABLE STANDARDS AND LEGISLATION

Data Protection Act 1998
Information Security – ISO27001