Data Protection & Privacy

Version Control

	Last Amended	Author	Reason for Amendment
1	16/11/2017	Charlotte Banks	Initial Release
1.1	02/02/2018	Charlotte Banks	Changes to Sections 5.1 & 5.3
1.2	09/04/2019	Charlotte Banks	Changes to Section 4.

1 Copyright

2 Document Information

Policy Owner	SSG	Policy Contact	Compliance Officer
Document Owner	Compliance Officer		
Purpose	Main Information Security Policy		
Related Operational Policies	IS 00 Information Security Policy IS 01 Information Security Management IS 02 Information Security Policy and Objectives		
Relevant Committees	MSG		
Relevant Legislation and Standards	Data Protection Act 1998 GDPR 2018 ISO27001 ISO27002 ISO9001		
Relevant codes of practice and guidance notes	Not applicable		
Monitoring/reporting requirements		Communication plan	
Monthly SSG Meeting		MSG Meetings Presentation to All Staff Central Electronic Repository Face to Face Email Awareness	
Distribution	All Staff	Introduced	25th April 2018
Review Period	Annual	Sign-off level	MSG

Table of Contents

3 Introduction

EnablesIT is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

The organisation has appointed a management steering group who take control of data protection. Their role is to ensure the organisation complies with its data protection obligations. They can be contacted via their representative at charlotte.banks@enablesit.com. Questions about this policy, or requests for further information, should be directed to this group via Charlotte Banks.

3.1 Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4 Data protection principles

The organisation processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner;
- The organisation collects personal data via informal checks and official checks (e.g. DBS and other verification methods) only for specified, explicit and legitimate purposes;
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- The organisation keeps personal data only for the period necessary for processing; and
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- The organisation as part of the recruitment process will undertake checks on publicly available information to verify an individual’s eligibility and suitability to work within the organisation.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal or legitimate basis for processing as per that above principles. It will not process personal data of individuals for other reasons.

Personal data is processed for the following reasons:

a. In order to perform the contract, you have entered into with them.
b. In order to comply with a legal obligation.
c. Where it is necessary for the company's legitimate interests (or those of a third party) and the individual's interests and fundamental rights do not override those interests.

In some cases, personal data may be processed for the following reasons:

a. In order to protect the individual's interests (or someone else's interests).
b. Where it is needed in the public interest.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the appropriate legislations on special categories of data and criminal records data.

Special categories of data and criminal records are processed for the following reasons:

a. In order to carry out the company's legal obligations or exercise rights in connection with employment.
b. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to an occupational pension scheme.
c. In limited circumstances, with the individual's explicit written consent.

The organisation will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.
Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

5 Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

5.1 Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the organisation will at its own discretion charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to charlotte.banks@enablesit.com. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

5.2 Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to the compliance office – charlotte.banks@enablesit.com

6 Data security

The organisation takes the security of HR-related personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7 Impact assessments

Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8 Data breaches

If the organisation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

9 International data transfers

The organisation will not transfer HR-related personal data to countries outside the EEA.

10 Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11 Training

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

12 This Policy

This policy is subject to review as part of the annual review by the Security Steering Group (SSG) and the Information Security Management System (ISMS).