Data Protection & Information Security Policy & Procedure

This is a non-contractual policy

Created: March 2020
Review Date: April 2023

Introduction

This policy outlines how you, as an employee of Smartdesc (the company) manage personal data within your role. It should be read in conjunction with the Data Protection Guidance document.

The company is committed to the protection of the personal data of employees and other individuals about whom it might hold information. The company recognises the EU and UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 as the primary statutory responsibilities relating to data handling and processing of personal data.

To this end every individual handling data collected or administered by the company must take responsibility and have due consideration for its appropriate use in line with this policy.

This policy applies to all employees and other relevant parties (hereinafter referred to as 'employees'). Any deliberate breach of this policy may lead to disciplinary action being taken, or access to company facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

Responsibilities

1. Employees

The company holds various items of personal data about its employees which are detailed in the staff privacy notice. Employees must ensure that all personal data provided to the company in the process of employment is accurate and changes to personal data are updated regularly on CitrusHR.

In the course of day to day working it is likely that employees will process individual personal data. Prior to handling any data, employees are required to have completed training in Data Protection. In addition, employees must maintain a current understanding of what is required of them under Data Protection law, this will be achieved through annual Data Protection training.

When handling personal data employees are required to follow the guidance set out in the Data Protection Guidance.

2. Managers

Managers must ensure that employees handling data in the course of their roles have undertaken the appropriate training, are processing data within the frameworks agreed and following the guidance set out in the Data Protection Guidance document.

Managers and staff members will look to identify weaknesses in information security in their day-to-day work. Where weaknesses are found, the Information Security Team should be notified so that action can be taken promptly.

3. Directors

The Directors are required to demonstrate ownership of this policy and to communicate its values across the company. This accountability cannot be delegated; however, operational aspects of data protection management may be delegated to others. They must gain assurance that these responsibilities are being fulfilled and ensure resources are available to fulfil the requirements of this policy and associated procedures. They have overall accountability for the strategy of the company and are responsible for strategic oversight of all matters related to statutory legal compliance and risk for the company.

4. The Information Governance Team

The Information Governance Team are responsible for the practical implementation of data protection legislation across the company and ensure that the principles of data protection law are upheld. They must provide assurance to the directors that the companies obligations under data protection law are met and advise the wider company on day-to-day data protection issues.

Compliance

1. Respecting Individuals' Rights

The GDPR sets out a series of rights for individuals. Employees planning data processing activities must record how these rights are addressed. The Data Protection Guidance details the rights and the company's standardised processes to meet these individual rights.

2. Processing Special Categories of Data

The company will only process special categories of data linked to individuals, such as:

- racial or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature
- trade organisation membership
- sexual life or sexual orientation
- genetic data or
- biometric data (where used for ID purposes)

with the consent of individuals except for where:

- there is another condition on which to process this data lawfully
- the information is required to protect individual health in an emergency.

This data may be analysed in broad terms where no direct link to an individual can be made.

3. Processing Health Related Data

The company will process information relating to individuals' physical or mental health in order to comply with health and safety, occupational health or other legal obligation and to undertake an assessment of employee capability.

4. Subject Access Requests

The Data Protection Guidance details the procedures on how Subject Access Requests must be handled. As standard, the company does not charge to comply with access requests and will refuse manifestly unfounded or excessive requests.

5. Data Breaches

The company will put in place processes to detect data breaches including audits and other appropriate processes. Where an employee discovers a data breach, they must report this to incidenthelpdesk@smartdesc.co.uk as soon as possible and in any case within 24 hours.

If you have been made aware of a data breach, please follow the Security Incident Procedure.

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a high risk to the rights and freedoms of individuals and could result in material harm. Where there is a high risk to the rights and freedoms of individuals they shall be notified directly also.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. A personal data breach can happen for a number of reasons:

- loss or theft of data or equipment
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- cyber attack
- deception of the company.

Information Security

1. Data Storage

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by employees in accordance with statutory, regulatory, contractual and company policy requirements.

The company uses a number of platforms for securely storing data online including:

- CitrusHR
- Egnyte
- Microsoft Office 365
- Dext
- Service Now
- Learning Management System

Employees are required to store data they handle on all of these platforms only as detailed within the Data Protection Guidance.

Explicit permission from line managers must be obtained before removing restricted information, including personal data and confidential information from company premises. Restricted information processed on portable devices and media must be encrypted. The password to an encrypted device must not be stored with the device.

Data storage applies in relation to hard copies, file notes, incoming and outgoing letter correspondence. We will ensure data is held securely. Provisions employees must put in place include:

- lockable filing cabinets
- a clear desk policy
- secure storage for archived files
- secure destruction, using a shredder or confidential waste bin.

The same requirements apply to electronically held data. Provisions employees must put in place include:

- use storage on our cloud systems or approved platforms
- Files containing personal data should be shared with other members of staff as links to files stored on Teams, where files need to be shared with external stakeholders SharePoint should be used..
- use of secure platforms for processing data
- up to date internet security systems and software (i.e. Bitdefender)
- secure destruction of IT equipment.

Employees are not permitted to use external storage devices such as external hard drives, memory sticks, pen drives etc. for storage of any company data other than for transfer of photos and data whilst on company premises.

2. Disposing of Data

The company is committed to keeping data for the minimum time necessary to fulfil its purpose. Full details of data retention can be found in the Retention Policy and Schedule.

Employee Data

The company will keep employment history data and health data to which long tail liability claims may refer for 100 years from the date of documentation in order to be able to verify employment details of former employee or assist with employers' liability claims. Most other data will be removed a minimum of six years after their employment with the company has finished, in order to meet data needs for pensions, taxation, potential or current disputes, or job references.

Health and safety data

The company will keep health and safety records of accidents that happen for three years after the date of accident, other than in the case of data to which long tail liability claims may refer in which case the company will retain the data for 100 years from the date of the accident in order to be able to assist with employers' liability claims.

Paper based records shall be disposed of in a confidential waste sack, confidential waste bin, or shredded. Electronic records will be deleted through the decommissioning of equipment by the IT department and digital records shall be deleted from databases at source.

3. Disposing of IT Equipment

Even if you think you've deleted data from your computer it's likely remaining somewhere in some form, so disposing of IT equipment securely is essential. You must contact the Procurement Manager to have IT equipment removed and disposed.

4. Email Security

Your email address is individually assigned to you and should not be shared with others. In your absence or for specific investigation purposes only emails may be accessed by authorised individuals. You should take the following steps to ensure the security of your emails:

- Use SharePoint as the preferred file sharing option, otherwise email. Consider whether the email content should be encrypted or password protected. If sending a spreadsheet containing personal data this must be password protected. The password should be delivered using an alternative method of communication e.g. Telephone or SMS.

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Dave" - the auto-complete function may bring up several people named "Dave". Make sure you choose the right address before you click send.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

- Never click on a link or share any information with anyone that you don't recognise - if in doubt check with the Information Security and Governance team or a member of staff with sufficient technological expertise.

5. IT Systems

Employees must undertake appropriate training to ensure sufficient security awareness and must make best attempts to protect their identity by using a strong password. Account passwords and usernames should not be shared without authorisation from your line manager and should only be shared through our password management system.

Remote Working

Where an employee works remotely from the premises, they shall ensure the adequate protection of the data to which they have access. This includes:

- keeping confidential and secure their access details (user name, password etc)
- protecting information from access by third parties (e.g. family, friends etc)
- password protecting documents, laptops, memory storage devices etc
- immediately reporting any breach or suspected breach of this policy to incidenthelpdesk@smartdesc.co.uk

Confidentiality

When working for the company, employees will often need to have access to confidential information which may include, for example:

- information about individuals who are members or otherwise involved in company activities
- information about the internal business of the company
- information about others working for the company.

The company is committed to keeping this information confidential, in order to protect people and the company itself. 'Confidential' means that all access to information must be on a "need to know" and properly authorised basis. Employees must use only the information they have been authorised to use, and for purposes that have been authorised.

Employees must assume information is confidential unless they know it is intended by the company to be made public. Employees must also not disclose confidential information to unauthorised people or cause a breach of security. In particular employees must:

- not compromise or seek to evade security measures (including computer passwords)
- be particularly careful when sending information to other agencies and organisations

- not gossip about confidential information, with colleagues or people outside the company
- not disclose information — especially over the telephone or electronically — unless they are sure of who they are disclosing it to, and that they are authorised to have it.

If in doubt about whether to disclose information or not, employees should not guess and should withhold the information while they check with the Directors whether the disclosure is appropriate and liaise with the Information Security and Governance team for advice on the method of disclosure. In accordance with employment contract terms and conditions, employees' confidentiality obligations continue to apply indefinitely after they have stopped working for the company.

Record Keeping

When a new employee joins, a personnel file for the storage of records relating to them is set up then scanned electronically. Employees' records may contain documents such as:

- personal details such as name, address, telephone number(s), email address, date of birth, marital status, emergency contacts, employment/contract dates, rates of pay, bank account details, entitlements, absence records (sickness, holiday, parental leave etc), national insurance number, health questionnaires, occupational health reports, TU membership etc
- job description
- performance review (appraisal)
- assessment records and observations, including test results
- qualifications including copies of any certificates
- training and development plans and objectives
- continuous professional development (CPD / CPC) records*
- training and development activities completed, including evaluation forms
- references, authorisation checks such as DBS, right to work in the UK etc.

*The company may store records of employees' CPD but is not responsible for their CPD record keeping requirements, as determined by professional bodies.

Policy Monitoring

The Information Security and Governance Team are responsible for the monitoring, revision and updating of this document on an annual basis or sooner if the need arises.

Security classification	OFFICIAL – NOT MARKED
Author	Andrew Coyle
Owner role	Head of Information Security
Approved by	Head of Information Security
Approval date	20/11/2019
Distribution	All staff via email and intranet. Staff induction
Signature required	No
Latest review date	25/04/2023
Next review date	25/04/2024
References	EU General Data Protection Regulation

	UK General Data Protection Regulation 2021 Data protection act 2018 ISO 27001 & ISO 27002 Information Security Standard and Code Of Practice

Change History

Version	Owner	Changed by	Change summary	Date
1.0	IT Director	Andrew Coyle, Smartdesc Associate	NEW	19/01/17
1.1	ISM	Andrew Coyle, Information Security Manager	Reviewed	17/04/18
1.2	ISM	Andrew Coyle, Information Security Manager	Reviewed and minor amendments	04/10/2018
1.3	HoIS	Ricci Wilding, Information Governance Officer	Reviewed and minor amendments	20/11/2019
1.4	HoIS	Ricci Wilding, Information Governance Officer	Reviewed and minor amendments	25/02/2020
1.5	HoIS	Ricci Wilding, Information Governance Officer	Reviewed and minor amendments	12/01/2021
1.6	HoIS	Kemi Emmanuel, Information Governance Officer	Reviewed and minor amendments	20/05/2022
2.0	HoIS	Ricci Wilding, Information Governance Manager	Amendments and brand change	25/04/2023