Scattergoods Agency Ltd

# Data Security Policy

## 1. INTRODUCTION

**1.1** The Company has adopted this Policy to comply with the Data Protection Legislation, which requires those who process Personal Data to adopt appropriate security measures and thereby prevent or reduce the risk of unauthorised disclosure, loss, theft or destruction.

**1.2** The objectives of this Policy are to:

- Comply with the Data Protection Legislation
- Protect the rights of the Data Subjects whose Personal Data we process
- Provide openness and transparency
- Demonstrate accountability in relation to the of data protection principles
- Take reasonable steps to protect the organisation from the risks inherent to processing Personal Data

**1.3** As a Data Controller, the Company acknowledges that it is granted a great deal of responsibility in handling the Personal Data, often without Data Subject's consent and for its own interests; as such we take our obligations to safeguard Personal Data while it is under our control seriously.

**1.4** This Policy sets out the general operational methods and restrictions to be adopted by all personnel to protect against Data Breaches.

**1.5** We acknowledge that Data Breaches may result from mistake, misconduct or improper use of the Personal Data we hold. Examples include:

- removing data (or a copy of data) from the Company's effective control
- failing to properly secure Company devices, including computers, phones and tablets
- accidental loss of Company devices
- malware or computer hacking
- failing to ensure correspondence is correctly addressed

**1.6** Please refer to the list of definitions at the end of this Policy to clarify terms used in this Policy.

## 2. OVERVIEW

**2.1** This Policy covers all Company Personnel.

**2.2** Company Personnel are required to adhere to this Policy in the course of their work for the Company without exception.

**2.3** Failure to comply with this Policy may result in disciplinary action and / or termination of the contract between the individual concerned and the Company.

## 3. GENERAL PROVISIONS

**3.1** **Sensitive Personal Data**: Company Personnel must exercise particular care and caution when processing Sensitive Personal Data and actively consider and act to prevent (or minimise the risk of) data breaches in this respect.

**3.2** **Copying**: Company Personnel must not send, receive, copy, photograph or otherwise duplicate any Personal Data held by the Company, and/or accessed during the course of their work for the Company, for any purpose that does not relate to their work duties and responsibilities.

**3.3** **Visitors:** Visitors to Company premises must be accompanied at all times. If you identify an unknown, un-escorted or otherwise unauthorised individual on the Company's premises you must immediately notify your manager, or another suitable manager. If no such manager is available, you must notify a Responsible Person.

**3.4** **Physical Security of Premises:** All Company Personnel have a shared duty to ensure that areas in which Personal Data is stored or accessed are physically secure, including:

- Filing cabinets that contain Personal Data must be locked when not in use and the key/s kept securely.
- All rooms on Company premises that contain servers, devices that are (or have been) used to store Personal Data, or any manual filing systems must be kept locked at all times other than when they are being accessed by authorised individuals

**3.5** **Clean Desk:** All Company Personnel shall keep a clean desk and ensure that printed materials containing Personal Data are not left unattended at their workstations.

**3.6** **Treatment of Personal Data:** Company Personnel shall not refer to or describe Personal Data (sensitive or otherwise) in public or using systems or channels of communication that are not under the control of the Company.

## 4. PASSWORDS

**4.1** Always use a secure password when accessing the Company's systems and ensure it meets the following standards:

- Passwords must be unique to the work setting (i.e. different form the passwords you use on personal devices).
- Passwords must not be stored electronically, either on work systems or your own personal devices.
- Passwords must be changed regularly, either as prompted by the systems in question or at least every three months.
- Passwords must not be shared with, or divulged to, work colleagues or any third parties.
- Passwords should be of at least 8 characters and contain both upper and lower-case letters, at least one number and at least one non-alphanumeric character.
- Passwords should be selected on the basis of a phrase that is memorable to you and not a word in English or any other language.

**4.2** Electronic documents that are sent as email attachments and that contain Personal Data, must wherever possible be password protected and the password be conveyed to the recipient by separate means.

## 5. DEVICES

**5.1** All devices used for work purposes must have full disk encryption enabled and firewall software activated.

**5.2** The Company's IT provider will also be familiar with the specifics of how encryption products function. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time, so it is also important to ensure encryption methods remain effective.

**5.3** You must not use personal devices to store, send or receive Personal Data that relates to your work with the Company. If you use a personal device for these purposes, or any other purpose that involves Personal Data obtained in the course of your work with the Company, you must report this without delay. Failure to do this may be dealt with as a disciplinary matter.

**5.4** You must notify a head of department or the Responsible Person immediately in the event that a device that contains Personal Data is lost, mislaid, stolen or damaged so as to render it inoperable.

**5.5** Employees who leave their employment or other work for the Company must return all Company devices upon which Personal Data is stored by the relevant termination date at the very latest.

**5.6** It is not permissible to use detachable storage devices to store Personal Data (e.g. portable hard drives, or USB sticks) except with the express prior approval of your manager or the Responsible Person. If any such device is to be used it must be encrypted.

## 6. BREACH REPORTING

**6.1** Any member of Company Personnel who becomes aware of a potential Data Breach, including any breach of this Policy, or learns of any facts which are indicative of a breach, or future breach, must notify the Responsible Person immediately. Data breaches will be dealt with under the Data Breach Policy and Procedures.

**6.2** A person who reports a suspected breach or potential breach will be protected as a whistle-blower and will not be subject to any detrimental treatment by or on behalf of the Company. Furthermore, all due process will be taken to protect against detrimental treatment by others.

**6.3** It is not up to members of staff to make judgments about whether or not circumstances amount to a breach of this Policy; if in any doubt you must report what you know to the Responsible Person.

**6.4** You may speak to your line manager and any other internal manager for guidance, however, the duty to report is to report in writing either to the Responsible Person directly, or to another suitable manager with the Responsible Person reading in copy.

## 7. REMOTE WORKING

**7.1** You may only work in locations other than the Company premises with the express prior approval from your line manager, or another manager with suitable authority, or if your contract with the Company provides for this.

**7.2** You may only work remotely on Company Devices and must take all reasonable steps to ensure the Company Devices used are secure, encrypted and password protected. The use of personal devices including mobile telephones, tablets and computers for work is strictly prohibited unless formally agreed, and subject to certain security measures being placed on your device, which may include encryption, password, or the installing of Company-approved applications.

**7.3** You must refrain from accessing Personal Data in any location which is not physically secure, such as a public place, restaurant, park etc.

**7.4** You must ensure any Company Device you use for remote working is securely locked away when not in use to avoid any theft or unauthorised access. You should also take care to avoid inviting theft, by for example leaving a device visible inside a car (locked or otherwise).

**7.5** Insofar as is possible, you must take care to prevent the screen of any Company Device from being visible to others.

**7.6** Do not connect any Company Device to any third-party network that has not been pre-approved by the Company. Do not use publicly available Wi-Fi services offered by businesses, and street 'hotspots' such as The Cloud, or BT-WiFi to access the internet. Instead access the internet using a 'tether' to a Company Device that is data enabled (such as a Company mobile phone).

**7.7** You should de-activate the bluetooth capability on Company Devices when in busy public places; bluetooth is vulnerable to attack and public areas are commonly targeted by hackers.

## 8. PROTECTION FROM MALWARE

**8.1** You must not open any email attachment which may pose a threat of malware content. Malware can often be distinguished with one of the following attributes:

- The sender is not identified by name but rather by email (e.g. the Company's system does not recognise the sender as being a person)

- The sender is not known to you in your work capacity
- The sender's identity is different or otherwise incompatible with their email address
- The email may be from someone you know, but contains a generic phrase that invites you to click on a weblink
- The email attachment is in a file format you do not recognise as a normal document file type (examples of normal file types include:'docx', '.pdf', 'xlsx', '.rft'.)
- The attachment is unusually large (1mb or greater)
- The subject line, or text of the email suggests that the attachment should not be trusted or that it is not work-related

**8.2** In any of these scenarios you must contact the Responsible Person and/or the IT department for advice and guidance on how to proceed.

## 9. RESTORING DATA FROM BACK-UP

**9.1** The Company's data will be backed-up regularly to a portable disk drive in addition to any automated back-up measures which store the content of servers at a remote location.

**9.2** The secondary back-up will be performed regularly by a Responsible Person, and will be stored securely on-site in a fire-proof safe and will not be taken off-site for any reason without the express written permission of the Managing Director.

**9.3** In the event of a major Data Breach resulting from loss or corruption of its servers the Company's data will be restored from its remote back-up [or by hard disk backup]. This may only be done by the Company's IT Department or IT Provider.

## 10. CORRESPONDENCE

**10.1** All new email addresses and other contact details must be verified prior to being used to send any items of Personal Data.

**10.2** When using email, you can verify the address by emailing the recipient without including any Personal Data and asking them to respond confirming something that only they should know. Alternatively you can do this by contacting the recipient by phone and asking them to spell out their email address in full to ensure it is accurate.

**10.3** Where correspondence includes Sensitive Personal Data (e.g. regarding any person's health or criminal convictions) you must take extra care to ensure the correspondence is sent to the correct address (either geographical or email). Hard copy letters that contain Sensitive Personal Data must be marked 'confidential' and addressed to a named person within the recipient organisation. If the correspondence is for someone in the Company, consider hand-delivering it to reduce the risk of a data breach.

**10.4** If you send reference requests to third parties (e.g. in relation to applicants for employment or worker contracts) you must take care to ensure the return address (email or geographical) is correct, the name of an individual to whom the response is to be sent is provided and the referee specifically requested to address the reply to this individual and to mark the envelope 'confidential'.

## 11. REDUNDANT COMPANY DEVICES

**11.1** Data stored electronically is very difficult to permanently erase, for this reason all devices that have contained work related Personal Data should be treated as continuing to store such data until such time as the Responsible Personal has confirmed they are safe for disposal.

**11.2** Measures taken to store such devices and restrict access to them must be at least as stringent as for other Company Devices.

## 12. SOFTWARE DRIVERS & PATCHES

**12.1** Often when systems are updated existing hardware items such as printers, scanners, etc require updated software drivers (or patches) to work correctly.

**12.2** Software drivers may only be installed and / or updated by the Company's IT department or IT provider; you should never attempt this yourself and must never use drivers downloaded from the internet for these purposes.

## 13. SOFTWARE – GENERAL

**13.1** Work systems only run Company approved software for good reason: each and every piece of software that operates on a Company Device creates the risk of a 'back door' attack on the Company's systems. For this reason, you may never install non-standard software on any Company Device.

## 14. TRAINING

**14.1** The Company will ensure that all Company Personnel receive suitable training on data security; if you are aware of any member of staff (employee, worker, temp, contractor, volunteer) who has not had this training you must report this to the Responsible Person without delay.

**14.2** If you feel you require more training to adequately operate within the Data Protection Legislation, please inform your line manager or the Responsible Person.

## 15. DEFINITIONS

**Company Personnel:** all employees, workers, contractors, agency workers, volunteers and consultants who are engaged to work for the Company.

**Company Device:** computer equipment including desktop, laptop and servers, mobile telephones, tablets, USB sticks and stand alone hard drives or other data storage devices.

**Data Breach:** an act or omission that compromises the security, confidentiality, integrity or availability of Personal Data, or a failing in the technical and organisational safeguards put in place to protect Personal Data. Any unauthorised access, disclosure, loss, damage or destruction qualifies as a Data Breach.

**Data Controller:** the organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR.

**Data Protection Legislation:** any applicable law or code of conduct which applies to the activities of the Company, which in the UK is the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018.

**Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data.

**Personal Data:** any piece of information which identifies a Data Subject, either directly or indirectly, alone or in combination with other data we can reasonably access, including any pseudonymised Data. Personal Data can be factual or consist of notes and opinions about a Data Subject. Any Personal Data that is processed by automated (electronic) means or as part of a structured filing system is covered by the Data Protection Legislation.

**Responsible Person(s):** the designated officer or officers within the Company who take responsibility for matters relating to Data Protection. In our organisation, the Responsible Persons are:

Karen Elson – karen@scattergoods.co.uk – 01483 461963
Darren O'Leary – darren@scattergoods.co.uk – 01483 461950

**Sensitive Personal Data**: highly personal information which Data Subjects are likely to consider private and which relates to:

- Race or ethnic origin
- Political opinions and religious or spiritual beliefs
- Trade union membership
- Physical or mental health
- Sexual life and orientation
- Biometric or genetic data
- Criminal offences and convictions