Data Protection

DOs & DON’Ts GUIDE
CONTENTS

PAGE 1 - CONTENTS

PAGE 2 - INTRODUCTION

PAGE 2 - YOUR ROLES AND RESPONSIBILITIES
  - FUNDAMENTAL ‘DOs’

PAGE 3 - WHY PROTECT PERSONAL DATA?
  - THINGS YOU CAN DO TO PREVENT SECURITY PROBLEMS

PAGE 4 - PASSWORDS
  - STORING PERSONAL DATA

PAGE 5 - SENDING AND SHARING PERSONAL DATA

PAGE 6 - EMAIL

PAGE 7 - FAX
  - TELEPHONE

PAGE 8 - CCTV

PAGE 9 - LAPTOPS, IPADS AND DESKTOP COMPUTERS

PAGE 9 - WORKING ONSITE

PAGE 10 - WORKING OFFSITE
  - DISPOSAL OF PERSONAL DATA

PAGE 11 - LOSS OR THEFT OF PERSONAL DATA (DATA BREACHES)

PAGE 12 - CONTACT DETAILS
Introduction

This document is a guide for any SIG employee who collects, manages, transfers or uses data about customers, employees or other individuals during the course of their work. The aim of this guide is to raise awareness relating to the safe handling of personal data. Following these rules will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation SIG plc might suffer from the loss of personal data.

Your roles and responsibilities

Everybody within SIG plc has a shared responsibility to secure any personal information used in their day to day professional duties and even employees not directly involved in data handling should be aware of the risks and threats and how to minimise them.

Fundamental ‘DOs’

- Ensure you have completed the relevant Data Protection Training;
- Follow the relevant procedures and guidance within the Data Protection Procedure Manual at all times;
- Remember that the Data Protection rules apply to paper files, data held electronically, video/DVD, audio files/tapes and photographs;
- Be particular careful when handling sensitive personal data i.e. concerning race, political opinion, religious beliefs, trade union membership, physical or mental health, sexual life or criminal offences as it needs to be treated with greater care than other personal data;
- Collect and use personal data only when necessary;
- Do your best to ensure personal data is accurate and up-to-date;
- When writing documents and emails containing information about another individual, remember that the individual in question has a right to see any information relating to them;
- Remember that even deleted emails may be retrieved and revealed to the individual they relate too – if you wouldn’t want them to see what you are sending then you should not send it;
- Raise any security concerns;
- Encourage colleagues to follow good practice and guidance;
- Report incidents when a loss, theft, unauthorised access, accidental or deliberate release of personal information has occurred.
Why protect Personal Data?

SIG holds personal data on customers, employees and other people to help them conduct their day-to-day activities. Some of this personal data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data can result in media coverage, a criminal conviction and potentially damage the reputation of the company.

The handling of personal data is everyone’s responsibility. Failing to protect data could amount to gross misconduct or even legal action.

Things you can do to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of personal data going missing or being obtained illegally. Many of these ‘dos and don’ts’ will apply to how you handle your own personal data and will help you protect your own privacy.

“Compliance with the Data Protection Act is essential to how we work and is a legal requirement”
Passwords

Do

- Follow SIG’s password procedure;
- Use a strong password (strong passwords are usually 8 characters or more and contain upper and lower case letters, as well as numbers and special characters);
- Make your password easy to remember, but hard to guess;
- Choose a password that is quick to type;
- Change your passwords if you think someone may have found out what they are;
- Change your passwords on a regular basis.

Don’t

- Write your passwords down;
- Save passwords in web browsers if offered to do so;
- Use your username as a password;
- Use names as passwords;
- Email your passwords or share them in instant messages.

Storing Personal Data

Do

- Store all removable media securely;
- Securely dispose of removable media that may hold personal data;
- Password protect all files containing personal data;
- Ensure hard copies of personal data are securely stored and disposed of when their retention period has expired;
- Ensure that hard copies of personal data are securely transported and stored when removed from the SIG premises and only do so where authorised.
**Sending and Sharing Personal Data**

**Do**

- Encrypt or password protect all files containing personal data prior to sending them electronically;
- Always send file passwords separately to the email the file is attached to;
- Be aware of who you are allowed to share information with. Check with the Data Protection Compliance Department if you are not sure;
- Verify an individual’s identity before providing any personal data relating to them;
- Ask third parties how they will protect sensitive information once it has been passed to them and confirm this in writing.

**Don’t**

- Send personal data (even if encrypted) on removable media (USB memory drives, CDs, portable drives) if secure remote access is available;
- Send personal data by email externally unless it is encrypted or password protected;
- Assume that third party organisations know how personal data should be protected.
Email

Do

- Double check the recipients email address, some email software will suggest similar addresses you have used before. Make sure you chose the right one before you click send;
- Use SIG’s contacts or your address book where possible. This helps to stop email being sent to the wrong address;
- Only use your SIG email account for work purposes.

Don’t

- Use personal accounts such as Yahoo or Hotmail for sending work related emails;
- Attempt to bypass SIG’s security measures to access your email offsite, for example forwarding email to a personal account;
- Turn off any email security measures that your IT team has put in place or recommended;
- Write any comments about an individual that is unfair or untrue that you would not be able to defend if challenged. You must assume that anything that you write about a person, even in informal e-mails, may be seen by that person;
- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal data, such as passwords or account details;
- Email personal data internally unless it is password protected;
- Email personal data externally unless it is password protected or encrypted. Contact the IT Service Desk for advice on encryption or password protection.
Fax

Do

- Consider whether sending personal data by a means other than fax is more appropriate;
- Make sure you double check the fax number of the recipient;
- Check that you are sending a fax to a recipient with adequate security measures in place;
- Ask the recipient to confirm they are at the fax machine, they are ready to receive the personal data, and there is sufficient paper in the machine;
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to view the contents;
- Telephone the recipient to ensure that the fax has been received.

Don’t

- Send personal data via fax unless absolutely necessary;
- Send a fax without using a cover sheet;
- Assume a fax has been received by the intended recipient.

Telephone

Do

- Inform all staff if call recording is in operation;
- Ensure that access to the equipment used to record calls is kept in a secure area and access is only granted to authorised personnel;
- Obtain evidence of a person’s identity prior to providing their personal data over the telephone.

Don’t

- Take credit card details using speaker phone facilities;
- Repeat credit card details back to callers;
- Provide call recordings without first contacting the Data Protection Department for authorisation.
CCTV

Do

- Display the appropriate signage at all entrance points to a building;
- Inform all staff if CCTV is in operation;
- Ensure that monitors displaying CCTV images located in reception areas are turned away so that they are only visible to staff;
- Ensure that access to the equipment used to retain CCTV images is kept in a secure area and access is only granted to authorised personnel;
- Ensure that the equipment used has the technical specification to ensure that the recordings are of a suitable quality;
- Ensure that recorded images are kept for no longer than necessary.

Don’t

- Provide CCTV image recordings without first contacting the Data Protection Department for authorisation;
- Position cameras in locations where they will capture images of an individual’s private property;
- Position cameras in locations that can capture images of Chip and Pin terminals or computer screens used for processing credit card transactions;
- Position the monitor used to view images in public view unless the monitor displays a scene which is also in plain site from the monitor location i.e. customers in a trade counter or employees in an open plan office can see themselves on a monitor screen. This is acceptable as they cannot see anything on the monitor which they could not see by looking around them;
- Use equipment capable of recording sound to record conversations between members of the public, this is classed as highly intrusive and is unlikely to be justified;
Laptops, IPads and Desktop Computers

Do

- Shut down your laptop using the ‘Shut Down’ or ‘Turn Off’ option at the end of each day or when taking a laptop offsite;
- Try to prevent people from watching you enter passwords or view sensitive information;
- Turn off and store your laptop/IPad securely, for example, if travelling always remove your Laptop/IPad from your vehicle when using overnight accommodation;
- Use a physical laptop lock if available to prevent theft;
- Lock your Desktop/Laptop/IPad when leaving them unattended (⌘ + L – Desktop and Laptop);
- Use good password practices e.g. never keep your ID and password details with your laptop/IPad.

Don’t

- Leave your laptop/IPad unattended unless you trust the physical security in place;
- Leave your laptop/IPad unattended in a vehicle unless absolutely necessary, in which case lock it away, out of sight, in the boot area of the vehicle;
- Leave your laptop/IPad in a vehicle overnight;
- Let unauthorised people use your Desktop/laptop/IPad;
- Use hibernate or standby.

Working Onsite

Do

- Lock personal data away when left unattended and at the end of each working day;

Don’t

- Let strangers or unauthorised people into staff areas;
- Disclose login IDs, PINs or other security information to unauthorised users.
- Position screens where they can be read from outside the room or by unauthorised individuals.
**Working Offsite**

**Do**

- Only take offsite personal data that you are authorised to do so and only if it is necessary for the performance of your employment role;
- Ensure that personal data is protected offsite in the ways referred to above;
- Wherever possible access information remotely instead of taking it offsite;
- Be aware of your location and take appropriate action to reduce the risk of theft;
- Try to reduce the risk of people looking at what you are working with, when processing personal data.

**Don’t**

- Write down or otherwise record any network access information;
- Disclose login IDs, PINs and other dial-up/VPN information to unauthorised users.

**Disposal of Personal Data**

**Do**

- Use a cross shredder or confidential waste sacks/bins for the disposal of documents containing personal data;
- Contact the IT Department to arrange for the disposal of all computer equipment used for the processing/storage of personal data.

**Don’t**

- Dispose of personal data in general waste or recycle bins;
- Leave confidential waste sacks unsecured e.g. overnight or unattended;
- Sell or donate obsolete IT equipment.
**Loss or Theft of Personal Data (Data Breaches)**

**Do**

- Report immediately to the Data Protection Department when a loss, theft, unauthorised access, accidental or deliberate release of personal information has occurred;
- In the event of a Laptop/IPad/IPhone/Blackberry being lost or stolen contact the IT Department to arrange for the equipment to be remotely disabled.

**Don’t**

- Assume that someone else has reported a loss, theft, unauthorised access, accidental or deliberate release of personal information has occurred.
Contact Details

SIG UK

For any Data Protection related questions, comments or issues, please contact the Data Protection Compliance Department at:

Data Protection Executive
Human Resources
Signet House
17 Europa View
Sheffield Business Park
Sheffield, England, S9 1XH
Email: dataprotection@sigplc.co.uk
Tel: 0114 285 6047

SIG Ireland

For any Data Protection related questions, comments or issues, please contact the Human Resources Manager at:

Human Resources Manager
SIG Building Products Ltd
Unit 42 O’Casey Avenue
Park West Industrial Estate
Nangor Road, Dublin 12
Email: dataprotection@sig.ie
Tel: 00353 1 6454 938