# DATA SECURITY & PROTECTION BRIEFING

**FOR NEW STAFF AND VOLUNTEERS**

## INTRODUCTION

*This is an introductory briefing on Data Security and Protection, intended for all new staff and volunteers*

In addition to reading this briefing, you are expected to undertake the online *Foundation Level Data Security and Protection* training course shortly after joining the organisation and annually thereafter. You will also need to pass a short assessment test every year to confirm your understanding of the training material.

This Briefing is only a start. After the training you should refer to the policies (details at the end of this briefing) and other material that will be published at intervals. Ask your line manager for details.

## DATA PROTECTION BASICS

### Personal Data and the Law

***Personal data** means any information relating to identifiable living persons (also known as a **data subjects**) who can be directly or indirectly identified by it*

Personal identifiers such as names, identification numbers, dates of birth, location data and online identifiers such as IP addresses can make data *personal*. Sometimes a combination of data items might make an individual's data identifiable where a single item on its own would not.

In the UK, the **Data Protection Act, 2018** and its **UK General Data Protection Regulation (GDPR)** largely control how **personal data** can be used by individuals and organisations.

Certain types of personal data are regarded as more sensitive and are legally classed as '**special category'**. More care must be taken in handling these types of data and processing them is subject to extra restrictions. The special categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Mental or physical health
- Sex life sexual orientation

## Processing

*When applied to **personal data**, the term **processing** simply means any handling or use of it*

Almost anything that can be done with personal data is counted by the law as processing. Examples include *collecting, extracting, storing, sorting, combining, converting, amending, encrypting, anonymising, pseudonymising, sharing, transferring, archiving, deleting …*

Everyone responsible for using personal data has to follow strict rules and abide by what are known as the '**data protection principles**'. There are seven of these principles, and they say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary
6. Protected by appropriate security
7. Processed in a way that demonstrates compliance with the principles

Your organisation has processes to help ensure that you follow the principles, but as an individual, you also have responsibilities.

## Your Responsibilities

*Everyone handling personal data has a personal responsibility for ensuring that it is processed fairly and lawfully*

- The organisation has Data Protection and IT security **policies** (see details at the end of this Briefing)
- The policies explain in more detail what you can and can't do with personal data - so familiarise yourself with them and abide by them
- You must co-operate in undertaking the Data Protection and the IT **training** provided
- You are individually responsible for the security of mobile phones, laptops, other IT equipment that you use in your work, even if you own it yourself
- You also have a key role as an individual in ensuring the **security** of personal data
- If you become aware of a security incident (or a near miss), you must report it immediately to the designated staff member so that it can be investigated and managed
- Remember, the purpose of reporting incidents is not to apportion blame, but to identify areas of risk and target training and other measures in order to improve our level of data protection
- It is important to understand who to go to for advice and guidance on Data Protection and IT issues, starting with your line manager
- Everyone needs to know how to recognise and report *Subject Rights* requests (see below)

## Subject Rights and Requests

***Data subjects** have a number of legal rights in relation to how their personal data is used to ensure that it is being processed legally and fairly*

These rights are the

- Right to be informed
- **Right of Access**
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Data Portability
- Right to Object
- Rights related to Automated Decision-making and Profiling

Data Subjects may make 'Rights requests'. The most common requests are based on the Right of Access to information and are known as **Subject Access Requests** or **DSARs - Data Subject Access Requests**. Individuals can always request access to the personal data about themselves that we are processing. They may also have the right to access data we are processing about the people they care for.

Requests can take any form - written or verbal. They can also arrive in all manner of ways. All are equally valid and need to be reported so that they can be checked and responded to within the tight timescales imposed by the law.

## CYBER SECURITY BASICS

***Cyber security** is how individuals and organisations reduce the risk and effects of cyber-attacks and deal with them when they occur*

This means being careful with the IT and data you work with to avoid breaches. It also means spotting problems and dealing with them promptly and appropriately when they happen.

Your organisation works with its IT suppliers to ensure that the IT **infrastructure is, and remains, secure.** In addition, there are many ways in which you as an individual can help further reduce IT risk and the possibility of breaches. These include:

### Passwords

- Create strong and memorable passwords e.g. by combining three random words
- Avoid using predictable passwords, such as dates, family, and pet names
- Don't keep written records of passwords
- Never reveal passwords to anyone - the IT team or IT provider will be able to reset passwords if necessary

### Email and Phishing

- Don't click on links or download files in emails unless you are expecting them and know where they have come from

- Look out for emails that include urgency or other ploys in an attempt to pressure you into doing something, possibly within tight time limits - give yourself time to think
- Report all attempts at phishing that you receive, whether they succeed or not
- Be careful when sending emails - it is too easy to send them to the wrong recipient.
- Do not send personal data by ordinary email - we can arrange for it to be sent securely by encrypted email
- Be especially careful when emailing or replying to multiple recipients as you can divulge email addresses inappropriately even when using the BCC facility

## Keep Your IT Devices Safe

- Don't ignore software updates. If prompted to install one, do so without delay
- Devices should be locked when not in use and need to be secured with a PIN, a password, or biometrically e.g. by fingerprint or face ID
- Avoid downloading fake apps. Check with your line manager and/or IT Supplier
- If installing apps is allowed, they should only be downloaded from an official app store such as Google Play or the Apple App Store

## When Things Go wrong

A personal data **breach** might occur in which personal data is:

- Lost or stolen e.g. by the loss of a device
- Destroyed or corrupted accidentally or maliciously
- Sent to the wrong person or organisation
- Divulged by accident
- Accessed maliciously via malware
- Accessed maliciously by another form of cyber-attack

**IT security breaches** can lead to personal data breaches, for example if a hacker gains access to stored data. Personal data breaches may need to be reported to the authorities and may also be breaches of data protection law.

**ALL**

**IT INCIDENTS, DATA BREACHES**

**AND NEAR MISSES**

**MUST BE REPORTED**

**AS SOON AS POSSIBLE**

## WHERE TO GO NEXT

| | |
|---|---|
| **Policy and guidance documents** | Stored in the: Data\SMT\Data Protection folder |
| **Data Protection email address** | dataprotection@ageukeastlondon.org.uk |
| **Data Protection Officer** | **Email**: dpo@exigia.com **Web:** https://exigia.com |

| Issue | Report to / contact | Notes |
|---|---|---|
| **An IT security or personal data incident (or near miss) has occurred** | Your Line Manager | • The Line Manager will inform the Director of Finance & Operations (DFO)<br>• The DFO will notify the Data Protection Officer (DPO)<br>• The DFO will inform the IT Supplier, *Penelope Technical*, as required<br>• The Line manager will update the Data Breach Register |
| **A subject access request has been received** | Your Line Manager | • The DFO will inform the DPO and together plan the response<br>• The DFO and DPO will liaise with the IT Supplier, *Penelope Technical*, to extract data<br>• The Line manager will update Data Breach Register |
| **A phishing email has been received** | Facilities Manager | The Facilities Manager will inform the IT Supplier, *Penelope Technical*, as required |
| **Advice on an IT problem or issue is needed** | IT Supplier | IT Support Email: support@wearepenelope.co.uk |
| **Advice on a data security / data protection problem or issue is needed** | Data Protection Officer | DPO Email: dpo@exigia.com<br>• New programmes<br>• Bids<br>• Complaints |
| **There is a new programme, bid or other potential use of personal data** | If you have access, complete a *DPIA Threshold Assessment Form*, otherwise, contact the DPO | Certain members of staff can access the DPIA Threshold Assessment Form by logging into by logging into https://exigia.com<br>DPO Email: dpo@exigia.com |
| **A request has been received from an external stakeholder (e.g. about a DSARs, policy or procedure)** | Requests can be received in various ways such as from a website link<br>A specified email account is monitored by the HR Manager, CEO, and DFO<br>An appointed person will deal with the request and consult the DPO as required | |