Supplementary Guidance

D&S IFCA Data Protection Policy

Standards on Information Security

April 2019

D&S IFCA Policy Documentation

Contents

Policy History

Version	Date	Comments
01	June 2017	Created by HR1
NJT 02	April 2019	Refined and updated by Neil Townsend (D&S IFCA)

1. Overview

The sixth principle of General Data Protection Regulation (GDPR) requires us to take appropriate technical and organisational measures to protect against the risks identified in relation to personal data – "Integrity and Confidentiality".

Good information security is **more** than just the physical protection of our information and equipment, (such as locking it away). It includes (as stated in the Information Commissioner's guidance):-

- Designing and organising it so that it fits the nature of the information we hold and the harm that may result from a security breach;
- Being clear about who is responsible for ensuring information security;
- Making sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained employees;
- Being ready to respond to any breach of security swiftly and effectively.

2. Assessing the Risks

We will take **appropriate** security measures to ensure that personal information and the equipment on which it is stored are kept secure and protected from unlawful and unauthorised processing (such as access, use, disclosure), accidental loss or damage.

To achieve this, we will

- Assess the levels of security that are required by taking into account:
    - The type of information that we are protecting (for example by increasing levels of security for sensitive information such as someone's physical or mental health details.
    - The threats and vulnerabilities to the information or equipment
    - The amount and nature of harm that may result from a security breach to the individuals whose information we hold (for example financial loss or distress).
    - The state of technological development at the time (what is available to protect the information or equipment)
    - The cost of implementing any measures

This risk assessment will also take account such factors as:

- The nature and extent of our organisation's premises and computer systems;
- The number of employees
- The extent of their access to the personal data; and
- Personal data held or used by a third party on our behalf (use of data processors).

3. Taking Appropriate Organisational Measures

This includes:

- Having up-to date Data Protection and Information Security policies that all employees are made aware of and agree to comply with. They are linked to disciplinary action in the event of breaches of the Data Protection Act and related legislation. These are all available on the shared server – Final Products/ Section D – Data Protection.

The development and implementation of an organised electronic filing system (Information Management System) that is supplemented by both a staff catalogue and a Data Protection Register.

By monitoring the internal systems and standards that have been introduced

By carrying out appropriate checks during recruitment to ensure that only those with appropriate discretion, honesty and integrity are appointed. For example, by taking up references and verifying information provided on job applications.

Ensuring our employees (including temporary ones, agency workers or individuals providing unpaid services to the Authority)

- Are fully aware of their responsibilities;
- Sign confidentiality agreements (where appropriate) before commencing work for us;
- Receive appropriate training, knowledge, guidance and support so they can effectively manage and protect the personal information that they have access to.
- Are reminded that personal information must only be accessed for the Authority's purposes, and not employees' private, personal or commercial use.
- Do not discuss an individual's information or affairs (such as one of our customer's) with family or friends, in public places or on social media.
- Ensure our service providers fulfil their security responsibilities where they have access to or are using information on our behalf, for example by requiring them to provide a written contract with security guarantees. **See our Standard on Ensuring Security in Procurement.**

4. Taking Technical Security Measures

Keeping information secure and protecting personal information from unauthorised or unlawful access, use or disclosure in practice means:

- Maintaining effective access controls such as restricted access on our networks on a strict need-to-know basis, and good password management.
- Protecting computers from viruses and other threats, by having up-to-date protection such as anti-virus, anti-spyware software, regular software updates and patches, and internet firewalls.

- Ensuring computers, laptops, smartphones and portable media such as memory sticks are password-protected and encrypted in case of loss or theft.

- Physical protection of computer equipment and filing cabinets, to prevent theft or damage, in the office, in transit or at home.

- Secure transfer of confidential and sensitive personal information by email using encryption of files where this is available, or use of secure networks.

- Maintaining a system of regular back-ups (including storing them off-site) and regularly testing their effectiveness.

Secure disposal of confidential and sensitive information by:

- Shredding and secure disposal of paper records;
- Destruction of computer media - eg by cutting up CDs
- Secure destruction of old computers and other storage media.

(There is guidance available on this from the Information Commissioner's Office on IT asset disposal for organisations)

- Maintaining up to date documentation of computer systems and programs.
- Keeping an up-to-date disaster recovery/business continuity plan and testing its effectiveness.

3.1 Process for Dealing With Data Breaches Taking

5. Dealing with Data Protection Breaches - Process

The Authority's process for dealing with data breaches such as security incidents, or suspected security breaches is:

That all data or personal information breaches of the GDPRD principle/s are reported to the Data Protection Officer, Chief Officer or Acting Chief Officer who will then liaise with relevant officers or Outsourced Services as appropriate.

Some examples of breaches that can occur are:

- Loss or theft of data or equipment on which data is stored (such as laptops, memory sticks, or smartphones)

- Inappropriate access controls allowing unauthorised use (for example using very easy-to-guess passwords or none at all).

- Hacking attacks

- Equipment failure (for example damage to a computer that results in corruption or loss of information that is not backed up).

- Human error (for example sending an email to the wrong distribution list, posting information to an incorrect address, or disclosing personal information over the phone without checking the recipient's identity first).
- 'Blagging' offences where information is obtained by people deceiving Authority employees.
- Unforeseen circumstances such as a fire or flood.

5.1. Containment and Recovery

We will ensure that all breaches are thoroughly investigated by the Data Protection Officer, Chief Officer or Acting Chief Officer and immediate urgent action is taken for containment, to limit damage caused, and prevent further data breaches. For example, we may isolate or close a section of our computer network, require employees to immediately change their passwords or change door entry access codes.

We will assess what we can do to recover any losses and limit damage caused for example by informing employees so that they are aware if someone tries to use stolen data to access information held by us.

Procedures are used to ensure (or highlight any actual or potential issues concerning) the maintenance of the integrity of electronic information, during and after an incident.

To ensure the integrity of electronic information is not compromised, we may temporarily use additional or third-party resources.

In some circumstances, the security breach may not appear to have affected the stored information. Checks will be made to demonstrate that the integrity of the information has not been compromised (for example by unauthorised access to information held on a network).

In order to ensure that recovery from a security breach that resulted in major equipment, environmental or personnel failure has been successful, procedures will be developed, tested, implemented and maintained. Such procedures will ensure that the integrity of stored information is not compromised during their implementation.

We will document situations where complete recovery from the results of a security breach cannot be assured, recording details of all actual or potential compromise to the stored information.

Where appropriate we will inform the police and other relevant organisations such as our information sharing partners if they may be affected by the breach.

5.2 Reporting

A written report is produced by the Data Protection Officer, Chief Officer or Acting Chief Officer. If serious breaches are identified, the Senior Leadership Team is notified.

The report describes:

- Details of the breach and findings such as what happened, who was involved, the circumstances, volume of data and who may be affected by it.

- The assessment of risk and potential harm, emotional distress and detriment that may be caused to individuals who may be affected by the breach.

We will take into account whether financial information (which may result in a risk of fraud or identity theft) or sensitive personal information was involved relating to their:

- the racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Recommendations (with timescales) for further remedial, preventative, and other action to be taken (for example for serious breaches, to notify the individuals affected and/or the Information Commissioner's Office).

- We may review and amend existing procedures to prevent other breaches and identify where improvements can be made.

Detailed Guidance and Forms for managing and reporting Data Breaches are available from the Information Commissioner's Office.

6. Home Working & Out of Office Security

We will ensure that personal information that is held or stored away from our offices is kept secure. The following security measures will be taken:-

- When in transit, computer equipment, accessories and papers will be locked away out of sight if unattended, for example in a car boot.

- Passwords will be protected and not disclosed or allowed to be on view.

- Documents and computer media should not be left lying around and desks should be cleared of any confidential information when no one is around.

- Equipment will be protected from accidental loss or damage. Care should be taken near computer equipment when consuming food and drink, or placing it close to it, in case of spillage which can cause damage to equipment and information.

- Make sure appropriate security measures are in place when sending confidential emails or transferring information.

- Firewalls, anti-virus and anti-spyware software must be operating at all times and be kept up to date.

- Family or friends should not be permitted to use Authority computers for private use, such as the downloading or playing of games. This can expose a computer to additional risks such as malicious computer programs or programs that may simply clash with software already installed. It may also result in unlicensed (and unlawful) software being operated on Authority computers.

- IT equipment (other than fixed desktop computers) will be locked away out of sight when not in use and will not be left on display.

7. More Information

Information Commissioner's Office: -	**Authority Codes of Practice & Guidance:-**
• Data Protection Guide – section on Information Security • Guidance on Reporting Data Breaches • IT asset disposal for organisations • A practical guide to IT security for the small business • Bring your own device (BYOD) – guidance on allowing use of personal devices to process personal data • Guidance on the use of cloud computing • Encryption – Advice on the use of encryption to protect personal data.	• Standard on Ensuring Security in Procurement

End.