Information Security Policy Suite

Information Handling Policy

includes Removable Media

ISPS-009

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Technology Services Management Team, to obtain a copy in a different format.

v

Approval Authority: {insert approval body here} Approval Date: xx/xx/2019

1. Purpose

The Council and its other public-sector partners hold a significant amount of information, much of which is very sensitive in nature about people and / or organisations.

1.1 Objective

The objectives of this policy are to protect the Council, individuals whose personal identifiable information we handle, and sensitive financial information from unauthorised disclosure, loss or theft by:

a. Establishing the Council's principles and accepted working practices in respect of handling information whether it is in the office, on the move, or at home.

b. Defining the distribution rules for information.

2. Scope

This policy applies to all staff, Members, partners, contractors and any other persons who have authorised access to the Council's information, information systems and networks.

This policy applies to all information held, created, modified or accessed from the approval date of this policy. It includes information in any form, no matter whether it is stationary (i.e. at rest) or in transit.

The Council has not adopted the TOP SECRET, SECRET or CONFIDENTIAL markings as it is highly unlikely that the Council will hold this information. Any information that is received that bears these markings should be referred immediately to the Technology Services Management Team (TSM) for advice, as they are outside the scope of this policy.

3. Policy Statements

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures that:

a. Are proportionate to the type and sensitivity of information being protected;

b. Protect information regardless of the information's current state:

b.1. Stationary (i.e. at rest)

b.1.1. Location, i.e. whether it is in Council buildings or at the home of an employee or Member. Sensitive information should only be stored within a physically secure environment.

b.1.2. Storage medium, e.g. network storage, paper, photographs, Digital Camera memory cards, USB sticks, etc. (see the entry for Removable Media in the Information Security Policy Suite's Glossary.

b.1.3. Sensitive personal information should never be stored on an unencrypted device.

b.2. On the move (i.e. In transit)

b.2.1. Unencrypted e-mails sent over the internet must not contain 'sensitive personal information'.

b.2.2. Papers containing 'sensitive personal information' must be stored and transferred in appropriately.

b.2.3. 'Sensitive personal information' should not be left in an unattended vehicle. It must be secured in a vehicle's lockable boot, where available, whilst on the move (i.e. in transit).

c. Incoming and outgoing mail points must be protected from unauthorised access and be physically secure, i.e. inside the secure perimeter;

d. Users must log off printers when not using.

3.1 Clear Desk Policy

a. Computers that are logged on to the network must be protected by locking the screen when not in use, e.g. when taking a break or attending a meeting.

b. Sensitive, business critical information must be securely stored out of sight when not required and especially when the office is vacated, e.g. in a lockable safe, cabinet or other form of security furniture.

3.2 Sharing Information

a. Unless there is a Data/Information Sharing Agreement in place with the Council, no third party (external contractors, partners, agents, the public or non-employee parties) may receive or extract information from the Council's network, information stores or ICT equipment. Such an agreement can be set up by issuing an instruction to the Legal Team.

b. Also see the Business Information Sharing policy (ISPS-008) and the Data Protection Policy (ISPS-011).

3.2.1 Publishing Information

a. Procedures must be in place to ensure that, where the Council has a duty to make information public, any personally identifiable information is redacted prior to publication (whether this is hard copy or electronic) unless there is legislation that allows the publication of some of this information.

b. Information on a publicly available system (i.e. on a Web server accessible via the internet) must be verified by the appropriate officer before publication. Care must be taken to protect the integrity of such published data to prevent unauthorised modification which could harm the Council's reputation or cause it to be in breach of the law, or other such rules and regulations.

3.3 Disposal of Information Policy

a. All hard copy records must be disposed of in accordance with the Data Retention Policy.

b. Papers that contain information that is personal, sensitive or carries a protective marking must be disposed of securely using the Council's authorised shredding facilities and / or services. They must not be put in recycling or household waste.

3.3.1 Disposal of electronic removable media

a. If no longer required, the previous contents of any re-usable media, e.g. Council Provided USB Sticks that are to be removed from the Council must be securely erased.

b. All electronic storage media, e.g. Council Provided Digital Cameras and Council provided USB Sticks that is no longer required, or has become damaged, must be returned to Technology Services for secure disposal.

c. The removal of all media from the Council can only be authorised by the Head of Service or a delegated officer and a record of all such removals to be maintained.

d. Auditable disposal of data storage devices must be securely destroyed in accordance with accredited data destruction standards and WEEE regulations, i.e. destruction certificate per asset.

e. Written procedures will exist for the disposal of all data storage devices including portable drives, laptops or any other electronic device capable of storing information.

4. Responsibilities

As per the Information Governance and Security Policy (ISPS-001)

Additional responsibilities arising from this policy are specified below.

4.1 Technology Services Staff

Their responsibilities include:

a. Ensuring that any electronic removable media issued is encrypted, where possible, before being issued to an individual authorised by the relevant IAO(s) for use.

4.2 Heads of Service

Their responsibilities include:

a. Ensuring that sensitive information is shared in a secure manner

b. Providing a business case to Technology Services authorising the use of removable media devices for any staff reporting to them that may have a genuine requirement to do use them.

4.3 Everyone (users / keepers)

Everyone is responsible to the relevant Head of Service for information asset handling. Their responsibilities include:

a. Only accessing systems and information, including reports and paper documents to which they are authorised.

b. Only using systems and information for work purposes.

c. Complying with any additional controls defined by the relevant Head of Service.

d. Ensuring that electronic files that are not part of a dedicated documents or record management system are:

    a. Saved in a shared location for those that require frequent access to the files, i.e. not on personal drives which prevents others from accessing them.

    b. Clearly named to reflect the protective marking and content of the files.

e. Ensuring that sensitive information is protected from view by unauthorised individuals.

f. Protecting information from unauthorised access, disclosure, modification, destruction or interference.

g. Only transferring information to Council-owned removable media, i.e. the use of personal USB sticks is unacceptable.

h. Copies of any information stored on removable media must also be stored on the source system or computer network until the information is successfully updated or transferred to another assured destination computer network.

i. To minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately physically secure and safe environment, see the Buildings, Infrastructure and Equipment Security Policy (ISPS-004).

j. Sensitive personal information should NOT be written or copied to unencrypted removable media.

5. Training associated with this Policy

As per the Information Governance and Security Policy (ISPS-001)

For further help and advice on how to securely use removable media devices log a call with the Service Desk.

6. Monitoring

As per the Information Governance and Security Policy (ISPS-001)

6.1 Non-compliance

As per the Information Governance and Security Policy (ISPS-001)

6.2 Review

As per the Information Governance and Security Policy (ISPS-001)

7. Equality Impact Assessment (EIA)

As per the Information Governance and Security Policy (ISPS-001)

8. Related documents

This policy should be read in conjunction with the following documents:

- ISPS-008 Business Information Sharing Policy;
- ISPS-011 Data Protection Policy;
- ISPS-001 Information Governance and Security Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures.

Appendix One – Data Sharing Considerations

These Data Sharing Considerations have been taken from the ICO Data Sharing Code of Practice and adapted for Horsham District Council use.

You will need to consider the following;

- **What Information needs to be shared? Does it contain personal data?**

  You shouldn't share all personal data that you hold about someone only the data that is required to achieve your objectives, e.g. You may only need to share their name and address, but not their date of birth.

- **Could the same objective be achieved without sharing any personal data or by anonymising it?**

- **Is there a Data/Information Sharing Agreement in place with the recipient of the data? If not please contact the Legal Team for assistance.**

- **Who requires access to the shared Data?**

  When sharing data, you should apply "Need to know" principles. This means that the recipient should only have access to our data, if they need it and then they also should only give access to that data to the relevant staff in their organisation to achieve the objective.

- **When should be shared and how often?**

  It is good practice to know and document this information, i.e. there are some circumstances where the data may need to be shared to achieve ongoing routine processes and other circumstances where it may only need to be shared once.

- **Where is the organisation that you are sharing the data with based?**

  If they are outside of the European Economic Area (EEA), the please contact the Legal Team for advice.

- **How should it be shared?**

  This involves the addressing the security surrounding how it is sent and/or accessed? If you require any assistance with this, please contact the Technology Services Team.