Security Classifications and Data Handling Policy

Version Control Sheet

Title:	Security Classifications and Data Handling Policy
Purpose:	To provide guidance for staff based on council policy.
Owner:	Data Protection Advisor lhenley@thurrock.gov.uk 01375 652500
Approved by:	
Date:	March 2019
Version Number:	1.0
Status:	Draft
Review Frequency:	As and when changes take place to security classifications.
Next review date:	As above.

Amendment History / Change Record

Date	Version	Key Changes / Sections Amended	Amended By

CONTENTS

1 MANAGING THE POLICY

1.1 Compliance:

All staff, members and contractors or others with access to council information must comply with this policy.

Anyone who is found to have breached this policy could be subject to the Council's Disciplinary Policy.

2 INTRODUCTION

2.1 From 2 April 2014 a new Government security classification scheme came into effect. This replaced the six classifications of:

- Unclassified
- Protect
- Restricted
- Confidential
- Secret
- Top Secret

2.2 The new scheme has three levels of classification and these are shown below:

- Official
- Secret
- Top Secret

The new classification scheme also includes data handling principles and these are shown in section 5.

The new classification scheme is not currently mandatory for Local Government; however this could change in the near future.

3 LEGAL FRAMEWORK

3.1 The revised classification scheme has been produced by the Cabinet Office and is compliant with the:

- Official Secrets Act 1989
- Data Protection Legislation
- Freedom of Information Act 2000 (and Environmental Information Regulations 2004)
- Public Records Act 1967

4 SUMMARY OF CLASSIFICATIONS

4.1 Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. The three levels of classification are:

4.1.1 OFFICIAL:

It is considered the majority of information that is created or processed by the public sector will be **OFFICIAL**. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile.

A limited subset of **OFFICIAL** information could have more damaging consequences (for individuals, the council or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the "**OFFICIAL"** classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the need to know. In such cases where there is a clear and justifiable requirement to reinforce the need to know, assets must be marked: "**OFFICIAL–SENSITIVE"**

4.1.2 SECRET:

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat factors. For example, where compromise could seriously damage military capabilities, internal relations or the investigation of serious organised crime.

Note - The council is unlikely to have any information which falls within the **SECRET** classification

4.1.3 TOP SECRET:

Her Majesty's Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Note - The council is unlikely to have any information which falls within the **TOP SECRET** classification.

4.2 IMPACT ASESSMENT / HARM TEST

It is the responsibility of the individual producing the document to assign Protective Marking. This individual is known as the 'originator', and is usually the author or owner of the document. The originator must decide on the appropriate Protective Marking classification for the document, based upon an assessment of the sensitivity of its content and the impact if the contents were compromised.

However as a rule of thumb, documents should be given a protective marking based on the premise of...

'...if this fell into the wrong hands, what impact and damage would it cause..?'

REMEMBER:

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business.
- Applying too low a protective marking may lead to damaging consequences and compromise of the information or person it relates to.
- If in doubt ask the Data Protection Team for advice.
- The protective marking of information should always be reviewed if subjected to a Freedom of Information Act enquiry.
- Protective marking can change during the life of a document or file. For example Contracts information could be OFFICIAL-SENSITIVE until negotiations are complete and then become OFFICIAL

5 PRINCIPLES

5.1 **Principle One**:

ALL information that needs to be collected, stored, processed, generated or shared to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection

5.2 The classification scheme applies to information (or other specific assets). Major ICT infrastructure (e.g. large aggregated data sets, payments systems, etc) may require enhanced controls to effectively manage associated confidentiality, integrity and availability risks – determined on a case by case basis following a robust risk assessment.

5.3 **Principle Two**:

EVERYONE who works with the council (including staff, contractors, councillors, partners and service providers) has a duty of confidentiality and a responsibility to safeguard any information or data that they access, irrespective of whether it is marked or not, and must have undertaken appropriate training.

5.3.1 Individuals are personally responsible for protecting any council information in their care and accidental or deliberate compromise of information may constitute a criminal offence. With this mind all staff must undertake the council's mandatory Data Protection Training.

All loss of data must be reported to the Data Protection Team or ICT Manager in line with the council's policies.

5.4 **Principle Three:**

Access to **SENSITIVE** information must **ONLY** be granted on the basis of a genuine 'need to know' and an appropriate personal security control.

5.4.1 Information needs to be accurate and available to the right people at the right time. Failure to share and utilise information can impede the effectiveness of the council. Taking into account Data Protection and confidentiality requirements, it is worth remembering that any recorded information can be requested under the Freedom of Information Act or Environmental Information Regulations, subject to exemptions, and published under Open Data.

5.4.2 The compromise, loss or misuse of sensitive information may have a significant impact on an individual and/or the council. Access to sensitive information must be no wider than necessary and limited to those with a business need. The 'need to know' principle applies wherever sensitive information is collected,

stored, processed or shared within the council and when dealing with external public or private sector organisations and partners.

5.4.3 The more sensitive the material, the more important it is to fully understand the levels of care needed to ensure its safe keeping. Some items will need additional security such as locked cupboards or other secure transmission methods.

5.4.4 Sharing this information internally should only be done on a 'need to know' basis. Sharing externally should only take place where there is an information sharing protocol, legal requirement, data protection request or approval sought from the Data Protection Team. Sensitive information must be shared where immediate action is required to protect life or stop serious crime.

5.5 **Principle Four**:

Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

5.5.1 The three protective markings indicate the sensitivity of information and the minimum personnel, physical and information security controls necessary to protect it.

5.5.2 The typical threat profile for **OFFICIAL** is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to protect council data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) activists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

5.5.3 The council is unlikely to have any information which falls within the **SECRET** and **TOP SECRET** classifications.

5.5.4 If any member of staff considers they hold **SECRET** information, please let the Data Protection Team know so that measures for the handling, despatch and destruction can be put in place.

6 OFFICIAL AND OFFICIAL - SENSITIVE CLASSIFICATION

6.1 OFFICIAL:

6.1.1 OFFICIAL is the classification which will apply to the majority of information created or held by the council.

6.1.2 All routine council business, operations and services should be treated as **OFFICIAL** and the council operates almost exclusively at this level. This includes:

- The day to day business of the council
- Public safety, criminal and enforcement activities
- Most aspects of security, resilience and emergency planning
- Commercial interests, including information provided in confidence and intellectual property
- Personal information that is required to be protected under the Data Protection Legislation.

6.1.3 **ALL** council information must be handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack. **Appendix 1** contains data handling guidance to help manage OFFICIAL information securely.

6.1.4 Staff must understand that they are **personally responsible** for securely handling any information that is entrusted to them in line with local business processes.

6.1.5 There is no requirement to mark **OFFICIAL** information.

6.2 OFFICIAL SENSITIVE

6.2.1 A limited subset of **OFFICIAL** information could have more damaging consequences (for individuals, an organisation or the council) if it were lost, stolen or published in the media. This subset of information should still be managed within the **OFFICIAL** classification tier but may attract additional measures to reinforce the need to know. When reinforcing the need to need to know the information must be marked **OFFICIAL- SENSITIVE.**

Managers will need to identify any sensitive information within this category. All information considered to be 'high risk' should be classed as **OFFICIAL – SENSITIVE**. For example:

- Where there is a bulk transfer of personal details.
- For certain commercial or market sensitive information which could prove substantially damaging to the council and/or a commercial partner if improperly accessed.
- For particularly sensitive personal information relating to an identifiable individual, where inappropriate access or disclosure could result in substantial harm or distress to an individual. For example, where relating to investigations, or vulnerable individuals.

6.2.2 When working with documents, classifications must be in CAPITALS at the top and bottom of each page. The classification of emails must appear in the subject field.

6.2.3 Data owners are responsible for identifying any information within this category and to put in place appropriate measures to ensure that this information is securely handled. To help with this some common sense data handling measures have been shown within **Appendix 1.**

6.2.4 Email rules are below:

- Internal and External emails containing **OFFICIAL** information can be sent via normal email (irrespective of who these are sent to e.g., police, resident)
- **OFFICIAL-SENSITIVE** emails that are sent internally must be classified as such and can be sent via normal email
- **OFFICIAL-SENSITIVE** emails that are sent externally (irrespective of who these are sent to) must be classified as such and sent via:
  - Your standard email address if the recipient is a public sector body (e.g. council, police, NHS etc.).
  - CitrixFileShare if the recipient is not a public sector body (e.g. resident, supplier).

6.3 Destruction

All council documents that are no longer required (check the council's Document Retention Policy) should be destroyed securely. There are a variety of methods by which this may be achieved, the most common of which is the use of council confidential waste bins.

APPENDIX 1 – Handling Information

The information below sets out standard control measures when working with information at **OFFICIAL** and **OFFICIAL-SENSITIVE** classification levels.

Important Notes:
The rules for **OFFICIAL-SENSITIVE** only apply when mentioned below, otherwise the rules throughout relate to the classification of **OFFICIAL**.

Personal Security:
- All staff to be Baseline Personal Security Standard cleared.
- All staff must complete the mandatory Data Protection training.
- Information Asset Owners and Managers must ensure access to **OFFICIAL-SENSITIVE** information is on a need to know basis.

Document/Record Handling:
- **OFFICIAL-SENSITIVE** records must classified as such.
- All staff when finished using a desk, or expect to be away for longer than 4 hours, must clear all information from the desk and ensure all paper work is locked away with the PC shut down.
- PC's must be locked when staff are going to be away from their desk for a short period of time, i.e. comfort breaks.
- All staff should give consideration to who needs access to **OFFICAL-SENSITIVE** data held and where to store it securely. There must be a business need to access this information.
- Information Asset Owners and Managers should regularly review who has access to **OFFICAL-SENSITIVE** information in their work areas.
- Managers should ensure when an employee leaves the team, their access is removed.

Storage:
- All staff should ensure that council data is only stored on the council's network or on a council issued encrypted device.
- Staff should ensure their area of the network has an appropriate file structure to support the retention of records in line with the council's Document Retention Policy.
- Council data stored on council issued portable media devices should be transferred to the council's network regularly to ensure that it is appropriately backed up.
- Laptops and other mobile devices must be protected from theft or unauthorised use when in transit and when used in remote locations.
- All staff should ensure they store manual records in a lockable cupboard.
- All staff should ensure that manual records are not accessed by staff or visitors to the council who do not have permission or a business need to access them.
- All staff should remain vigilant and challenge unfamiliar personnel/individuals within their working environment.

Remote Working:
- All staff should ensure they give consideration to their environment before working remotely.
- Staff must take precautions against being overlooked when working in transit or working from home. Consider using a privacy screen if regularly working in these environments.

- Do not remove **OFFICAL-SENSITIVE** records whether in hard copy or electronic form from a secure environment unless absolutely necessary. All records must be kept secure when not in use and locked away.
- Ensure the council's secure waste bins are used for disposal – do not use domestic waste bins.

Moving Assets by Hand:
- Consider whether it is appropriate to anonymise the data to protect client privacy/confidentiality.
- Do not remove significant volumes of records containing personal information whether in hard copy or electronic form from a secure environment unless authorised.

Moving Assets by Post/Courier:
- Ensure the envelope is suitably addressed, and contains the correct return address for items that cannot be delivered.
- Consider double enveloping for **OFFICIAL-SENSITIVE** information.
- Consider the use of recorded delivery or courier delivery for **OFFICIAL-SENSITIVE** information.

Moving Assets Overseas (by hand or post):
- Consider using recorded delivery or other commercial couriers who can vouch for the integrity and provide a chain of custody for the duration of the postage.

Bulk Transfers:
- Do not remove significant volumes of records containing personal information whether in hard copy or electronic form from a secure environment unless authorised.

Electronic Information at Rest:
- All data must be stored on the council's network.
- Data stored on portable devices must be on approved encrypted portable devices.

Electronic Information in Transit:

- Internal and External emails containing **OFFICIAL** information can be sent via normal email (irrespective of who these are sent to e.g., police, resident)
- **OFFICIAL-SENSITIVE** emails that are sent internally must be classified as such and can be sent via normal email
- **OFFICIAL-SENSITIVE** emails that are sent externally (irrespective of who these are sent to) must be classified as such and sent via:
    - Your standard email address if the recipient is a public sector body (e.g. council, police, NHS etc.).
    - CitrixFileShare if the recipient is not a public sector body (e.g. resident, supplier).
- Consider whether it is appropriate to anonymise the data to protect client privacy/confidentiality.

Removable Media (containing data):
- Device control has been implemented to ensure that data can only be removed from our network onto authorised devices.

- Council data stored on council issued portable media devices should be transferred to the council's network regularly to ensure that it is appropriately backed up.
- All staff should ensure that council data is only stored on the council's network or a council issued encrypted device (memory stick and/or laptop)

Telephony (mobile and landline), Video Conference and Fax:
- **OFFICIAL-SENSITIVE** information should not be sent via fax.

Disclosure:
- Official Secrets Act (OSA) and criminal cases subject to damage tests - Before releasing data of this nature staff must consult Legal Services.

Disposal / Destruction:
- Staff must ensure they dispose of documents in line with the council's Document Retention Policy.

Incident Reporting:
- All staff have an individual responsibility to report a breach. Breaches of security must be reported to the Data Protection Team or ICT Manager.
- The Data Protection Team will report any such incidents to the Council's Senior Information Risk Owner (SIRO) as appropriate.
- The Data Protection Team will risk assess all breaches and will notify the Information Commissioners Office (ICO) and other relevant bodies as and when required.