Information Classification and Marking Policy

Contents

1. Overview / introduction

Information classifications and markings are used to help you to identify information which may require extra care when handling, sharing or disposing of it.

If information is of a particularly sensitive nature (eg where its loss or disclosure would have particularly damaging consequences for individuals or groups), it is important to be able to identify it easily so that it can be protected appropriately.

This policy explains how you must classify and mark information so that the Council can fulfil its legal and regulatory obligations to keep sensitive and personal information secure.

1.1. Why is this important?

All staff and other users of the Council's ICT services have a duty to protect the systems, information and data that they use. There is an equally important duty to share information appropriately where this is in the interests of service users (eg where sharing information with partners in health or the police will protect the wellbeing of individuals).

Correctly classifying and marking information (so that more sensitive information is easily identifiable), and following clear, common sense instructions for the way that information is handled, are essential for helping us fulfil this responsibility. This also helps to ensure that services are able to use and share information effectively (both internally and also with partners) to deliver high quality public services.

Applying too high a classification can inhibit sharing and lead to unnecessary and expensive protective controls. At the same time, applying too low a classification may result in inappropriate controls and potentially put sensitive information at greater risk of compromise.

We also have to meet legal and regulatory standards on information security, including:

- General Data Protection Regulations
- Data Protection Act
- Freedom of Information Act
- Environmental Information Regulations
- Caldicott review: information governance in the health and care system
- Cabinet Office guidance on the information classification and marking scheme for government, including:
    - Government Security Classifications
    - Guidance on working with OFFICIAL information
    - Guidance on working with personal information
- Common law duty of confidence
- Specific statutory obligations of confidence (eg medical confidentiality, health and safety)

If we don't protect the information we use or if we fail to comply with legislation, people and services could be put at risk. We could also face substantial fines and our access to essential data that is shared with us by partners and agencies could be taken away.

If you don't comply with this policy, you may be subject to disciplinary action under the Council's Code of Conduct (refer to the Council's Disciplinary procedure for details of this).

1.2. Audience

This policy applies to all:

- Councillors
- permanent staff
- temporary staff (including contractors and consultants)
- third parties accessing the Council's ICT resources (including suppliers, partners, staff working in shared service arrangements, work-experience staff, students)

2. Responsibilities

We are trusted with handling sensitive and personal information from a range of citizens, staff, partners and suppliers. This means we have a responsibility to store, share and dispose of it in a safe and secure way.

This policy explains your duties and obligations for classifying and marking information that you have access to so that it is protected appropriately. It also outlines related Council policies and procedures which you need to comply with.

2.1. Requirements

To protect Council data and information, you **must**:

2.1.1. Make sure you understand and comply with this policy and any other policies, guidelines or legislation specified within it when accessing, handling or sharing information or data.

2.1.2. Make sure that any information or data that you or your team are responsible for is correctly classified and marked in accordance with this policy.

2.1.3. Make sure any staff you manage or third parties you have responsibility for (i.e. by sponsoring their access) are:

- aware of and follow this policy
- suitably trained and have any relevant resources made available (eg appropriate equipment, secure disposal facilities etc)
- provided with, and understand, any changes or updates to this policy

2.1.4. Make sure any service processes and information sharing agreements you are responsible for comply with this policy.

2.1.5. Alert your manager if you believe there has been a breach or potential breach of this policy. The process for reporting a breach can be found on the intranet.

2.1.6. Contact the Council's ICT service if you have any questions about this policy or how to comply with it.

2.1.7. Be aware of and comply with the following policies and procedures:

- the Council's Using Systems and Data Policy
- information handling protocols within your service area
- the Council's procedures for data protection, including reporting information security breaches
- the Council's records management policies and procedures
- all relevant information sharing agreements when handling data belonging to a third party organisation (eg government department, police, NHS partner etc) - this includes any classification and marking requirements defined in such agreements
- other relevant policies which relate to your area of work, such as those relating to the Regulation of Investigatory Powers Act (RIPA)

3. Classifying information

Information classifications indicate the sensitivity of information and level of risk that its loss or inappropriate disclosure might bring.

This policy explains how you must classify information so that it can be protected appropriately.

3.1. Requirements

To keep the Council's information and data secure, you **must** be aware that:

3.1.1. **All information handled by the Council is classified as OFFICIAL by default**, even if it is not marked as such. The security controls for OFFICIAL (eg pre-employment checks, building access and technical security arrangements) are based on commercial good practice, with an emphasis on all users to respect the confidentiality of all information.

3.1.2. A smaller amount of OFFICIAL information is of a particularly sensitive nature and access needs to be more tightly controlled. This varies from service to service and applies to information where loss or disclosure could:

- result in significant harm or distress to an individual or group
- cause a significant financial impact to an individual or group
- substantially damage the reputation of an individual, group, the Council or partner organisation
- enable criminal activity to take place
- prejudice a criminal investigation or legal proceedings

For this information an additional 'handling instruction' of 'OFFICIAL-SENSITIVE' must be used so that the importance of only sharing it on a strict 'need to know' basis is reinforced to anyone who receives or is given access to the information.

OFFICIAL-SENSITIVE is **not** a separate classification. Instead, it is used to mark a subset of OFFICIAL information for the purpose of emphasising the higher level of sensitivity of the information. This is recognised across government and its use helps to ensure that information that is shared with other government departments and agencies is appropriately handled.

3.1.3. Information shared by partner organisations will be subject to their own classification, marking and handling policies (eg NHS, police etc). See section 5 of this policy for details and requirements for information classification and marking when working with partners.

3.2. Examples

3.2.1. Examples of information that is classified as OFFICIAL include:

- general and routine correspondence
- most personal data, including care and financial records (high risk cases with special handling requirements may meet the criteria for classification as OFFICIAL-SENSITIVE - see below)
- replies to Freedom of Information (FOI) requests
- ongoing and / or general reporting and management information
- routine discussion of some aspects of security matters
- policy development and advice to Council members (except on contentious and very sensitive issues)
- minutes of meetings

3.2.2. Examples of information that should be considered as OFFICIAL-SENSITIVE include:

- very sensitive personal information about vulnerable or at-risk people where loss or disclosure could lead to significant harm or distress
- large volume data (eg bulk sets of care or financial records)
- information about criminal investigations and legal proceedings that could

compromise public protection or enforcement activities, or prejudice court cases
- the most sensitive corporate information (eg organisational restructuring or negotiations, and major security or business continuity issues)
- policy development and advice to Council members on contentious and very sensitive issues
- commercially or market sensitive information that might be damaging to the Council or to a commercial partner if improperly accessed

4. Marking information

Information classifications help identify information which may require extra care (eg additional technical or process controls) when handling, sharing or disposing of it. This policy describes how you must mark information in order to protect it and keep it secure.

4.1. Requirements

When working with the Council's information assets (including email, documents, files, forms, letters, faxes, handwritten notes etc), you **must**:

- be aware that ALL Council information is classified as OFFICIAL by default, and does not need to be explicitly marked as such
- mark sensitive or high-risk information as OFFICIAL-SENSITIVE to indicate that extra care needs to be taken when handling it
- make any classification markings clearly visible by adding them to the:
    - header and footer of documents, spreadsheets or presentations
    - subject line of emails
    - filenames and folders for electronic records
    - front of folders or binders for paper records

5. How our partners classify and mark their information

Since the introduction of the Government Security Classifications Policy (2014), the public sector has been working to adopt the OFFICIAL classification and marking scheme. However, some partners may continue to use previous classification and marking schemes. This means it is important that you are aware of these when you work with partners so that you can handle information they share with you in line with any information sharing agreements that are in place.

The table below shows how the new government classifications map to the former government scheme and NHS classifications.

New government classifications	Old government classifications	NHS classifications [1]
OFFICIAL	UNCLASSIFIED	NHS Unclassified

[1] The NHS uses the Caldicott Principles when handling information (including adult social care records) that identify an individual.

(plus additional 'SENSITIVE' handling instruction where required)	PROTECT	NHS Protect
	RESTRICTED	NHS Confidential

5.1. Requirements

When working with partners' information assets (including email, documents, files, forms, letters, faxes, handwritten notes etc), you **must**:

- be aware of the classification and marking used by partners for the information that they share with you
- comply with all relevant information sharing agreements when handling data that belongs to a third party organisation (eg government departments, police, NHS partners etc)
- ensure that information sharing agreements that you enter into on behalf of the Council clearly define how information that is shared must be classified, marked and handled (including defining any specific technical and procedural control requirements)

6. Applying this policy to your work

The Council's services handle a wide range of different information assets, and it is essential that appropriate classification and marking is applied so that the Council can fulfil its legal and regulatory obligations to keep sensitive and personal information secure.

6.1. Requirements

To apply this policy to your work and your team's work, you **must**:

- ensure that any information you create, access, share, store or dispose of is handled securely and protected in line with both the Council's Using Systems and Data Policy and guidance provided on the Council intranet
- ensure that any business processes that you are responsible for, and which involve routine handling of information classified as OFFICIAL-SENSITIVE, are reviewed in order to:
    - identify any additional technical and procedural controls that may be required to ensure that more sensitive information is appropriately secured
    - ensure that business processes and controls are properly documented and signed off by the Information Asset Owner, the Head of the shared ICT service and the Council's Senior Information Risk Owner (SIRO) [2]
    - ensure that all users, including partners, are aware of the required business processes and provided with appropriate training, guidance and support

[2] Refer to the Council's Information Governance Policy and Framework for further details of these roles.

7. Version history

Version ref	Author	Comments	Approvals		
			AfC	RB Kingston	LB Sutton
1.0	Rob Miller	Original version		16 May 2016	13 May 2016
1.1	Mark Lumley	Review as part of GDPR		05 April 2018	23rd April 2018