Information Security Classification Procedure

1. Introduction

This procedure provides advice on how best to maintain the confidentiality, integrity and availability of Council information assets by selecting the appropriate classification which will determine appropriate handling instructions and controls (for storing, processing and transmitting in a manner appropriate with the sensitivity of content and format of storage).

The sensitivity level of a data asset is commonly known as 'the classification'. The classification is based upon the severity of impact that unauthorised access to, destruction of, or the loss of confidence in the reliability of the data, would have on the Council, its employees and members of the public.

The classification directly relates to the handling instructions and any special handling controls to ensure the protection of the data asset. These methods provide guidance on how the data asset should be handled and secured during its lifecycle within the Council, up to and including its destruction.

All Council information which is defined to include personal, special category or business sensitive information requires careful handling in order to meet legal or contractual obligations. When this threshold is defined, information is allocated the classification label of **OFFICIAL-SENSITIVE**.

2. Legislation, Codes of Practice and Standards

2.1 In the event of an apparent conflict of handling or security instruction occurring between

a. Council Policy, Sharing Agreements or Professional Codes of Practice, staff must apply whichever instruction meets the higher security standard.

b. Legislation must take priority.

2.2 In the event of an apparent conflict occurring, staff should bring the matter to the attention of the Information Security and Digital Risk Officer (ISO) through their line manager, to ensure council procedures are reviewed and amended if required.

3. Roles and Responsibilities

3.1 Everyone who handles, or processes Council information is responsible for ensuring controls are in place for its continued protection in line with Council policy including:

- The Chief Executive (as Senior Information Risk Owner (SIRO)), the Head of ICT and Digital Enablement, the Information Governance Officer and the Chief Officer – Legal and Procurement. have corporate responsibility for the security of information;
- Business managers are responsible for operationally owning information, understanding what information is held, how it is used and transferred, who has access to it and why.
- Departmental responsible persons, such as system administrators, delegated to be responsible for specific information e.g. a database or file, are responsible for regularly reviewing user access rights and ensuring the lowest level of access is provided to users.
- All users are responsible for the manner in which they handle and process information to ensure its continued security

3.2 Managers must:

a. Identify what information used within their Department is to be marked as **OFFICIAL-SENSITIVE**.

b. Ensure processing is undertaken in compliance with data protection law. Guidance can be provided from the Information Governance Officer.

c. Take appropriate steps to ensure staff are made aware of what information is designated as **OFFICIAL-SENSITIVE** and provide staff with training and awareness of the working practices to be followed. This must also be communicated to non-ERC individuals and third party organisations such as agency staff, consultants, work experience students, volunteers or organisations processing or storing Council information on the Council's behalf e.g., providing a support service using client information provided by the Council or where the Council stores information on a server owned by another organisation. The preferred method of communication is via the ERC Information Security Sharing Agreement.

d. Provide regular reminders to staff of the handling instructions (at least once a year) where **OFFICIAL-SENSITIVE** is applied.

e. Be able to provide evidence of who has and has not been informed of information security and data protection policies and received training in both.

f. Ensure staff are supplied with the right equipment to meet the chosen handling instructions (for example providing lockable storage, encrypted USB devices, sturdy briefcases, document wallets or portfolios to safely carry information assets).

3.3 Staff must:

a. Ensure they are aware of and apply the handling instructions associated with the information they handle.

b. Alert their line manager if they believe an instruction is not adequate; where equipment provided is inadequate or where instructions conflict with those from other sources such as Sharing Agreements, Contracts or professional Codes of Practice.

c. Clearly mark files and emails as **OFFICIAL-SENSITIVE** where necessary (using the M365 prompt or manually typing it in capital letters).

4. Information Requiring Classification

4.1 The **OFFICIAL** marking indicates the information is below the threshold for **OFFICIAL-SENSITIVE** therefore typical duty of care practices are sufficient when handling that information.

4.2 The **OFFICIAL-SENSITIVE** marking indicates the information is **business sensitive** or would be classed as **personal** or **special category** under Data Protection law. It must be classified, and visibly marked where appropriate, ensuring that the classification is immediately visible.

4.3 **OFFICIAL-SENSITIVE** marking indicates protective action is necessary and applies to:

- PERSONAL and SPECIAL CATEGORY information, as defined by the data protection law. It is important to note that the identification of an individual is required. For example a name or other identifying factor is documented along with other details such as address, phone number, details of services being provided or medical conditions.

- OPERATIONAL information where there is an expectation of a 'need to know' for example, details of security practices or of how the Council reacts to a civil emergency or details of Council budgets or tenders which are pending approval.

4.4 Personal and Special Category Definitions

Information relating to a living individual that is Personal or Special Category information and falls under GDPR and the Data Protection Act 2018 (data protection law). Be wary though, a name is not the only way to identify a person so exclusion of the name does not automatically mean it is not Personal. A postcode tied with a rare medical condition could single out an individual for example.

At a very high and generic level, the following table shows personal and special category data.

Personal	• **Personal** (names, addresses, contact details, age, gender, birth details, physical descriptions, NI number, personalised vehicle number plates, passport number, student number, education grades)

	• **Family** (marriage, partnership or marital history, details of family & other household members, habits, hosing, travel details, leisure activities, membership of charitable or voluntary organisations) • **Employment** (employment & career history, recruitment & termination details, attendance record, health and safety records, performance appraisals, training records, security records, payroll or User ID) • **Financial** (income, salary, assets and investments, payments, credit worthiness, loans, benefits, grants, insurance details, pension info) • **Goods or services** (goods or services supplied to a person, licences issued, agreements and contracts • **Expressions & Opinions** - any expression of opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual • **Digital Footprint** – digital identities such as avatars, handles, gamer ID's, email address, login name, IP Address, Geo-tracking and location-based services.
Special Category	• Racial or ethnic origin • Political opinions • Religious or other beliefs of similar nature including philosophical beliefs • Trade union membership

	• Physical or mental health (medication) • Sexual preferences, sex life and/or sexual orientation • Criminal convictions or proceedings and criminal outcome & sentences • Offences (including alleged offences) • Genetic and biometric data for the purpose of identifying an individual (fingerprints, retina scan, voice signature, facial geometry)

5 Marking Documents

5.1 When documents are generated which contain **OFFICIAL-SENSITIVE** information, they must be marked. This does not apply to documents or emails that are generated externally for example, a letter sent to the council by a customer or a Doctor.

5.2 Where there is an automated prompt for marking documents, follow the prompts and select the classification that applies to the content of the document or email.

5.2 In the absence of an automated prompt, **OFFICIAL-SENSITIVE** information must still be marked. Staff are required to mark documents manually as follows:

a. Word, Excel or PowerPoint documents - add **OFFICIAL-SENSITIVE** to the header and/or footer of each page.

b. Email - add **OFFICIAL-SENSITIVE** to the subject header. If responding to an email that is classified by the originator, then only add your own classification statement if you have added information to the reply that requires **OFFICIAL-SENSITIVE** to be used.

c. Paper - either stamp or handwrite the classification level at the top and bottom of each page. As few staff create a handwritten document, it is not anticipated that this method would be needed often.

d. Databases – databases are often used to generate bulk communications for example Council Tax. Information printed from these databases will only be marked where the system itself is capable of labelling it. If the database has the functionality but does not use the term **OFFICIAL-SENSITIVE** an alternative indicator such as CONFIDENTIAL, ADDRESSEE ONLY would be acceptable.

e. Additional/Alternative Markings - Letters to customers and other agencies should only be marked with additional/alternative markings where it is already common practice to use one for example HR often use the label ‘Personal’, ‘Confidential’ or ‘Private’ or social workers notifying a client of support treatment might mark it as ‘Personal & Confidential’.

Use of these additional/alternative markings is at the discretion of the Department but if used, Departments must:

- document the terms that may be used;
- define why and when they can be used;
- make the instructions easily available for staff to refer to.

f. Blank Forms – Where it is known that a blank form, once completed, will be OFFICIAL-SENSITIVE, it can be beneficial to insert a classification rather than classifying it when the form has been received as complete. Consider adding “OFFICIAL-SENSITIVE when Complete” to the header and/or footer in advance.

g. Other – It may not be possible to directly mark some forms of information but alternatives should be considered for example, photographs (mark on the back),

video (mark on the casing), voice recordings (state what it is at the start of the recording) or backup tapes (mark on the casing).

5.3 Exceptions

5.3.1 Where a manager believes that their staff face exceptional circumstances which mean they will be unable to fully comply with handling instructions, they must first raise the matter with a Senior Manager and discuss what alternative options exist bearing in mind that just because something which has always been done in a particular way does not meant that it is still relevant today. If the Manager agrees there is no alternative, then they must submit a request for an exception to the ISO.

5.3.2 Managers are strongly advised to review working practices first, in order to determine if local operating practices change be changed to remove the need for an exception.

5.3.3 If the ISO approves the request, additional protective measures may be required. Departments must ensure that these are implemented locally as indicated.

6 Council Classifications

6.1 The Council uses three classifications, these being:

- NOT OFFICIAL
- OFFICIAL
- OFFICIAL-SENSITIVE

6.2 Classification Examples

The following are examples of the type of information for each classification; please note that the lists are not exhaustive.

NOT OFFICIAL

This covers information that does not relate to council business or day to day operations. This may include information such as:

- E-mail to colleagues advising of cake being available in the break room;
- A poster on a noticeboard advertising a lunchtime walking group; and
- E-mail to colleagues advising of a birthday card to be signed.

OFFICIAL

This covers routine business operations information This may include information which would be disclosed in response to a Freedom of Information Scotland Act (FOISA) request, but which the Council does not wish to publish pro-actively and would not want to release in an uncontrolled and out of context manner.

Information is restricted to staff or other contracted persons working on behalf of the Council. This may include information published on the Council's Intranet site and Council policies:

- Letters to staff, clients, parents etc. containing general information;
- Responses to FOISA requests;
- Internal directories and handbooks;
- Presentations;
- Agendas, discussion papers and meeting notes;
- Training materials;
- Routine budgetary details;
- Business cases; and
- Responses provided to Scottish Government for Parliamentary Questions.

Letters containing a name and address would be handled as Official however the addition of other identifiable data may require an increase in classification to Official-Sensitive.

OFFICIAL-SENSITIVE

This covers business sensitive information, personal or special category data under DPA 2018 (GDPR). It is shared on a need to know/named basis.

They key aspect of OFFICIAL-SENSITIVE is that unauthorised disclosure, (even within the Council), would cause harm to the interests of the Council or other parties by virtue of financial loss, loss of opportunity or reputation or cause embarrassment, harm or distress to individuals.

Personal and special category examples:

- Personnel records;
- Staff health records;
- Job application forms;
- Paper assets containing personal or sensitive data such as disclosure applications, housing application forms etc.;

- Individual payroll data;
- Customer/client personal details;
- Client health information; and
- Criminal conviction or alleged conviction information disclosed during security checks.

Business sensitive examples:

- Strategic plans;
- Commercially confidential information relating to suppliers;
- Planning and resource allocation information prior to final decisions;
- Investigations of alleged or suspected fraud;
- Misconduct or irregularity;
- Access codes and passwords;
- Tender submission details;
- Budget plans;
- Complaints;
- Operationally sensitive issues which may include presentations or discussion papers; and
- Some operational procedures would also fall into this category, particular those related to security measures.

7 Understanding other Classification Schemes

7.1 Where information is shared with other Public Bodies or third parties, it is imperative that an understanding of Classification schemes between organisations is present. One way to achieve this understanding is to use a recognised scheme as a basis of providing this cross-reference. Use of the Government Security Classification Policy to provide this cross-reference is recommended which relate to ERC as follows:

Government Classification	**ERC Classification**
Official	OFFICIAL
Official “accompanied with a descriptor”	OFFICIAL-SENSITIVE
* Secret	NA
* Top Secret	NA

* It should be noted that Local Authorities would not process Secret or Top Secret Information as defined within the Government Security Classification Policy. If this did occur, the minimum measures would reflect the Council's OFFICIAL-SENSITIVE classification and further guidance should be sought from both the Information Security and Digital Risk Officer.

8. Further Information

8.1 For more information about information classification or mapping to a scheme used by another agency, contact Ross Cowan, Senior ICT Officer (Cyber).

Document Control

Title	Information Security Classification Procedure
Prepared By	Cathie Fraser, Information Security and Digital Risk Officer, IT Services
Subject	Information classification and protective marking
Description	Provides guidance on maintaining the confidentiality, integrity and availability of Council data assets, by storing, processing and transmitting them in a manner appropriate with the sensitivity of content and the format of storage
Source Location	IT Services I:\ drive.
Reviewed By	Information Security Forum (ISF)
Published Location	Intranet
Classification	OFFICIAL
Review Frequency	Every 2 years

Version Control			
Version	**Date Issued**	**Author**	**Update Information**
2.0	Nov 2019	Cathie Fraser	Updated from existing guidelines. Accepted by CMT and ISF.
3.0	Aug 2024	Ross Cowan	Updated from M365 Classification and Retention Project.