



Protective Marking Policy

1. Introduction

This is Glasgow City Council's **Protective Marking Policy**. It is based on the Government Security Classifications Policy (GSCP) which came into effect in April 2014.

It sets out the basis by which information will be classified to **make sure** its sensitivity, integrity and availability is maintained throughout its life, particularly in terms of when it is communicated or transmitted. All documents **must be** classified and marked to show how sensitive the contents of the document are. This classified marking then decides what level of protection **must be** applied to the document.

2. Scope

This policy applies to all information assets (including both paper and electronic documents) created by or used within the council, but it is especially relevant and important for employees who deal with sensitive information concerning members of the public, employees or council operations.

The Head of Information and Data Protection Officer is available to give advice on what constitutes sensitive information and how it can best be protected. The CGI Service Desk **should be** contacted with any queries relating to IT aspects of this policy.

This policy is binding on all council staff and recommended good practice for all staff in council ALEOs.

3. Review

This policy will be reviewed on an annual basis and updated as appropriate, to **make sure** that it remains accurate and useful.

The **Information Security Board** is responsible for the review and the approval of changes to this policy.

The council's **City Administration Committee** is responsible for the formal approval of council policies and the delegation of specific tasks to officers.

The **Director of Governance and Solicitor to the Council** is the designated Senior Information Risk Owner for the Council and has a specific delegated power to issue (after appropriate consultation) binding Procedural Rules on the management of information. This Policy has been issued as such a Procedural Rule/Legal Precedence.



For the avoidance of doubt, and in the event of an apparent contradiction occurring between legislation, policy or best practice guidelines, legislation **will take** priority. This also applies to any future legislation that may be enacted.

4. Help with this policy

If you require help to apply this policy, first discuss the matter with your line manager. If required, please contact your Information Security Board representative.

5. Protective Marking classifications

The council Protective Marking Policy is based on the Government Security Classifications Policy (GSCP) which includes the following core categories of information classification:

- **OFFICIAL**
- **OFFICIAL-SENSITIVE**

It should be noted that GSCP also includes the categories '**SECRET**' and '**TOP SECRET**' but **will not** feature in the council Protective Marking Policy. This is because these categories tend to relate to matters such as national security and international relations and **do not** apply to any information routinely handled by the council.

GSCP defines '**OFFICIAL**' as "the majority of information that is created or processed by the public sector. 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 threat profile.

However, if certain categories of information that the council handles, were lost, stolen or published in the media there could be more damaging consequences for individuals, an organisation or the council itself. These categories of information normally require additional safeguarding measures and should be classed as **OFFICIAL-SENSITIVE**.

If something is marked **OFFICIAL-SENSITIVE**, a descriptor must be added to indicate what the sensitivity is, and, as a consequence, to restrict the availability of the information. The council has therefore developed the following descriptors,

- **OFFICIAL-SENSITIVE: PERSONAL DATA**
- **OFFICIAL-SENSITIVE: COMMERCIAL**
- **OFFICIAL-SENSITIVE: OPERATIONAL**
- **OFFICIAL-SENSITIVE: SENIOR MANAGEMENT**

In addition, it is recognised that staff will exchange or communicate information that may not strictly meet the definition of **OFFICIAL** or **OFFICIAL-SENSITIVE**, and so the council Protective Marking Policy includes,



➤ **NOT OFFICIAL**

Staff will still be required to determine that **NOT OFFICIAL** is the appropriate marking to use, but unlike **OFFICIAL** and **OFFICIAL–SENSITIVE**, there is no physical requirement to mark documents in this way.

The **full protective marking classification** which will be adopted in the council is therefore:

- **OFFICIAL – SENSITIVE: PERSONAL DATA**
- **OFFICIAL – SENSITIVE: COMMERCIAL**
- **OFFICIAL – SENSITIVE: OPERATIONAL**
- **OFFICIAL – SENSITIVE: SENIOR MANAGEMENT**
- **OFFICIAL**
- **NOT OFFICIAL**

The council has purchased an IT system called Boldon James Classifier which will be installed on every user's PC, laptop or tablet that connects to the Corporate Network - for use with MS Office and MS Outlook files. For documents created in these IT systems, Classifier **will force** users to select the appropriate marking to be applied to the document before it can be saved or transmitted.

Classifier will place a physical representation of the mark in the centre of the header and footer (footer only for Powerpoint) and will populate the document's properties table (not Outlook). Users should therefore take this into account when deciding to include other information in the document header and footer.

6. Relationship to other policies

This policy is one of a series of connected policies on the management and protection of information and should be read alongside those other policies. Key related policies are set out in Appendix 1.

7. Guidance

To accompany this policy various support documents are available on [Connect here](#). They include:

- **Staff Quick Guide to Protective Marking**
- **Staff Full Guide to Boldon James and Protective Marking**
- **Government Security Classifications Policy (GSCP) – Protective Marking Guide from April 2014**

Further information can be obtained by contacting your Information Security Board representative [here](#).



Appendix 1: Related policies and guidance

This Policy is one of a series of connected policies on the management and protection of information and **should be** read alongside those other policies. Key related policies are as follows:

- **Information Use and Privacy Policy** sets out the high level principles the council will adhere to when using personal data relating to our service users.
- **Information Security Policy** – this sets out the council’s high level approach to managing information security.
- **Information Risk Policy** – this sets out the approach by which the council will provide assurance that information risks are being managed.
- **The Acceptable Use of ICT Facilities Policy** sets out what staff are and are not allowed to do with council-issued IT equipment.
- **Information Security Guidelines** – these provide practical guidance and rules for staff on how to keep information secure.
- **Guidelines for staff using text and email** - to comply with core policies.