1. Introduction

This is Glasgow City Council's **Protective Marking Policy**. 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 classification 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. Relationship to previous, other protective marking schemes and implementation

The policy adopted by Glasgow City Council is based on the Government Security Classifications Policy (GSCP) which officially came into effect in April 2014. This has replaced the Government Protective Marking Scheme (GPMS), which had been widely used in central government, the police and many public authorities to protectively mark their own documents and information.

Staff should familiarise themselves with the new Government protective marking scheme to **make sure** that they can recognise sensitive documents and to reduce the risk of data leakage.

Although there is no requirement to re-classify information containing protective marking applied under the previous policy based on GPMS, the benefit in using a nationally-adopted standard is that we can safely receive GSCP protectively-marked documents and treat them just as we would our own documents with the same marking. Similarly, we can release our own protectively-marked documents to other agencies using GSCP and know that they will know how to protect them properly. This is not the same as saying we can share any information with any other body by using GSCP. There still needs to be a legitimate business need before any such release can take place, and legal advice should be sought before any new types of information release or exchange are agreed to.

6. Brief description of the new categories

The council policy is to adopt the Government Security Classifications Policy (GSCP) which includes the following core categories of information classification:

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

As with the former GPMS, 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.

The new rules do however recognise that a limited subset of '**OFFICIAL**' information could have more damaging consequences (for individuals, an organisation 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', information assets should be conspicuously marked: '**OFFICIAL–SENSITIVE**'.

If something is marked **OFFICIAL–SENSITIVE** then it is also permissible to add a "descriptor" to this 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 populate the properties table of the document with the selected mark and where relevant, will place a physical representation of the mark in the centre of the document header. Users should therefore avoid using the centre position of the header for other document information as it will be overwritten with the protective marking.

7. 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.

8. Guidance

To accompany this policy various support documents are available on Connect. 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.

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