RM-05 2021

The Scottish Parliament
Pàrlamaid na h-Alba

The Scottish Parliamentary Service

Protective marking system

The Scottish Parliament
The Scottish Parliamentary Corporate Body
The Scottish Commission for Public Audit

Introduction

A protective marking system is a common baseline for safeguarding information. A marking is applied to information to identify the standard procedures that are adopted in relation to its storage, security, distribution and disposition. A protective marking scheme safeguards information that needs to be protected by establishing handling procedures and business rules.

All employees of the SPCB should be aware of their responsibilities in relation to the use of SPCB information. Employees who handle protectively marked information should be particularly conscious of their personal responsibility for ensuring that their handling complies with the requirements of this system as well as the staff handbook.

> "In discharging your duty of confidentiality to the SPCB as your employer, you must exercise due care and diligence in handling information to which you have access as an employee. You must not disclose or comment on any information which carries a protective marking to any third party, either internal or external to the Scottish Parliament." Staff handbook – Code of conduct

Purpose

Protective marking is the method by which the originator of information indicates to others the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the Parliament and its ultimate method of disposal. To ensure that the Scottish Parliament's information assets:

- are marked and secured correctly
- are protected from inappropriate or unauthorised access, amendment or disposition

Some information is protected because its compromise may cause harm. The range of means by which harm could be caused to assets can be broken down into four general groups:

- disclosure
- theft
- destruction
- tampering

For further guidance, please refer to the Harm test in Appendix A – deciding if a protective marking is required

Protective markings

SPS staff are authorised and trusted to access protectively marked information should there be a business requirement. The SPS's protective marking system consists of two components to mark and restrict access to information:

- **Restricted** – can be applied to all information regardless of format and informs those with access to the information how it should be managed. All SPS staff can access restricted content for genuine business reasons.
- **Confidential** – can be applied to all information regardless of format and offers an additional layer of security by restricting access to information to predefined groups. Only those staff given access through membership of a group or through direct access should access Confidential information.

Restricted markings

It is the responsibility of the originator to apply restricted markings. All security cleared SPS employees, agency staff and seconded staff can apply Restricted markings.

Restricted markings, and appropriate descriptors, are used to identify rules for handling marked information. Staff should only access Restricted information if they have a legitimate business reason for doing so. Inappropriate access may be considered a breach of the *Acceptable use of IT policy* and may therefore be dealt with in accordance with the *SPCB's disciplinary procedures*.

When considering whether a Restricted marking is necessary, staff should apply the Harm test (Appendix A). Only in circumstances where the compromise of the information will cause harm, can a protective marking be applied.

Restricted markings should highlight information that needs to be managed to prevent unauthorised access, amendment, distribution or disposition. Only SPS employees, agency staff and seconded staff can apply or change markings.

Restricted - audit	Information concerning the adequacy and effectiveness of internal control processes.
Restricted - commercial	A commercial company's affairs, tenders under consideration or terms of tenders.
Restricted – in confidence	Information provided to the SPS in confidence and not for wider consumption.
Restricted - financial management	The finances or financial situation of the SPCB or MSPs.
Restricted - honours	Nominations for honours or awards.
Restricted - investigation	Investigations into complaints, disciplinary or other matters.
Restricted - legal privilege	Communications and information concerning legal advice.
Restricted - management	The management of SPS activities.

Restricted - parliamentary business	Parliamentary business.
Restricted - personal	Information identifying a living individual
Restricted - policy	New or changed policy before publication.
Restricted - private paper	Private committee business (Committees only)
Restricted - security	Security of individuals and property.
Restricted - senior management	The management of SPS activities by senior members of staff.
Restricted - staff	Information affecting the interests of staff.

Confidential markings

It is the responsibility of the originator to apply Confidential markings. A Confidential marking is a warning that the information has additional requirements and needs more rigorous management, including limiting who has access to it, than Restricted information. Access to Confidential information is limited to specific groups identified by [ ] e.g. *Confidential - senior management [Leadership]* indicates that access is limited to individuals within a group entitled *Leadership*.

Confidential markings should only be applied in circumstances where the compromise of the information will cause serious harm (see harm test).

Confidential - audit	Information concerning the adequacy and effectiveness of internal control processes.
Confidential - commercial	A commercial company's affairs, tenders under consideration or terms of tenders.
Confidential – in confidence	Information provided to the SPS in confidence and not for wider consumption.
Confidential - financial management	The finances or financial situation of the SPCB or MSPs.
Confidential - honours	Nominations for honours or awards.
Confidential - investigation	Investigations into complaints, disciplinary or other matters.
Confidential - legal privilege	Communications and information concerning legal advice.
Confidential - management	The management of SPS activities.
Confidential - parliamentary business	Parliamentary business.
Confidential - policy	New or changed policy before publication.
Confidential - security	Security of individuals and property.
Confidential - senior management	The management of SPS activities by senior members of staff.
Confidential - staff	Information affecting the interests of staff.
Confidential - variable	Variable access determined by user applying marking on a case-by-case basis.

Applying protective markings

Applying a protective marking to information indicates its value in terms of the damage that is likely to result from its compromise. To help prevent this happening the protective marking used indicates the type of controls needed to protect it.

Before applying a protective marking the harm test should be applied to determine whether or not a marking is necessary. For information on the criteria that the information must meet before a protective marking can be applied, please refer to Appendix A – deciding if a protective marking is required.

Handling marked information

Protectively marked information should be handled sensitively and according to the rules set out in Appendix B - Handling marked information.

Sharing protectively marked information

Should there be a need to share information subject to a protective marking, additional steps may be required to protect it.

Internal sharing using SP Online and Outlook

No additional steps are required when sharing protectively marked information internally within SP Online and Outlook in addition to the application of a sensitivity label. However, the use of attachments is not permitted - links should be used to share protectively marked documents and records within the SPS to maintain an audit history of activity.

Additional guidance on how to share protectively marked information internally by other means is detailed in Appendix B - Handling marked information.

External sharing using email

Email is the most common method used by SPS staff to share information.

Restricted information
When using email to share restricted information outwith the SPS, at least one of the following should be considered (in addition to applying a relevant Restricted sensitivity label):

1. **Default transit encryption** - the SPCB uses Transport Layer Security (TLS) (when supported by recipients) to protect sent emails, regardless of the protective marking. TLS is a strong encryption protocol designed to protect communications on the internet. TLS encryption secures e-mail in transit, preventing interception by third-parties. If in doubt, confirm with the recipient if their email systems support TLS. This level of encryption may be sufficient for

the majority of restricted marked information where the recipient e.g. Scottish Government, can be trusted and additional levels of encryption are excessive. There is no encryption applied following receipt of the information – the recipient is able to access and distribute further without limitation.

2. **Sharing agreement** - for regular planned sharing, e.g. for an event or project, with an external organisation or body, a sharing agreement should be in place. Prior to any agreement being signed, confirmation of the recipient's ability to support TLS encryption should be obtained. In most instances, default transit encryption and a sharing agreement combined are sufficient controls for protecting shared protectively marked information. A template sharing agreement is available on the intranet.
3. **Encryption** - where additional steps are required e.g. when the information being shared is considered special category personal information or highly sensitive security information, the protectively marked data should itself be encrypted by using encryption or other techniques or tools for sharing information externally advised by IMG and BIT.

Confidential
Confidential information (with a Confidential sensitivity label) sent from Outlook is encrypted (and not intended for an external audience). The sharing of Confidential documents externally is not permitted – the recipient will not be able to access it because of the applied encryption. Changing a Confidential marking to Restricted is permissible to make sharing possible should all steps be taken to ensure the protection of the information being shared.

Additional guidance on how to share protectively marked information externally is detailed in Appendix B - Handling marked information.

External sharing using online sharing tools

The SPCB only permits the use of BIT-supported tools for the sharing of protectively marked information. Under no circumstances should other online tools i.e. Dropbox, Google Docs etc. be used.

The external sharing features of SharePoint Online (Office 365) make it possible for SPS staff to share content with people outside the SPCB (such as partners, contractors etc.).

SPCB external sharing SharePoint sites
SharePoint Online sharing sites can be used by business areas where there is a need to share Not protectively marked or Restricted information outwith the BIT network. A sharing agreement should be in place for all instances of sharing protectively marked information with external parties using this method.

Using other organisation's sharing SharePoint sites
SPS staff may be required to upload SPS documents to external organisation's SharePoint Online (Office 365) repositories. Should there be a need to regularly upload protectively marked information to these locations a sharing agreement should be in place.

Sharing with Members

No additional steps are required when sharing Restricted information within SPCB systems e.g. using official email accounts. Members do not have access to internal SPS systems which will require you to share protectively marked documents and records using email attachments. Protectively marked information should not be sent to personal email addresses.

Members cannot access Confidential information.

Personal information

When sharing protectively marked information subject to data protection legislation externally (Restricted – personal or Restricted – staff), a data protection privacy impact assessment (DPIA) and data sharing checklist or agreement must be completed prior to any sharing activity.

For further information, please refer to the Data sharing section of the Data Protection intranet pages.

Distributing information with external markings

Should information sent to SPS officials be subject to external protective markings it is important to ensure that SPS protective markings are applied and that such markings are commensurate to the original marking when redistributing this information. Documents and records with the UK Government Security Classification ***Official*** should have the SPS ***Restricted*** security marking applied. Should the information received carry another externally assigned security marking, or a UK Government Security Classification other than ***Official***, staff should consult the Information Manager.

Disclosure of information

Protectively marked information may be made available only to those authorised. However, this does not affect any obligation that may arise to disclose information in response to requests in line with the requirements of the General Data Protection Regulation, the Freedom of Information (Scotland) Act 2002 or in compliance with other legislation or an order of the court. Following disclosure under FOI any markings should be removed.

For further information concerning disclosure, please refer to Appendix B - Guidance on dealing with protectively marked information

Archiving with NRS

Historical records selected for transfer to National Records of Scotland (NRS) for permanent preservation generally have all protective markings removed prior to transmission. The Freedom of Information (Scotland) Act 2002 allows individuals to request and receive information from Scottish public authorities, subject to certain exemptions. A number of these exemptions fall away at the point at which a record becomes a 'historical record'.

The vast majority of records transferred to NRS will be open to public viewing following transfer and should therefore have any protective markings removed. Should any FOISA exemptions still apply, the records will be transferred to NRS on a closed basis. Refer to *RM-04 Records management procedures* for further detail.

Breaches

Staff have a duty to ensure that all protectively marked information is securely stored and managed and that any transmission of such material is handled in accordance with this Protective marking system. Staff also have a duty to inform the SPCB of breaches. Failure to do so may constitute a breach of Parliament security rules and may result in disciplinary action. For further information, please refer to the *Data Protection policy* and *Security – protection of documents, equipment & personal items*.

Associated information

Information security policy
Acceptable use of IT policy
Data Protection policy
Security – protection of documents, equipment & personal items

Appendix A – Deciding if a protective marking is required

Step 1	Step 2	Step 3
Harm test The compromise of information would likely:	**Select marking and descriptor**	**Apply marking and descriptor**
Not protectively marked		
• not breach statutory restrictions on the disclosure of information • cause only minimal inconvenience on disclosure	Not applicable	No action required
Restricted		
• cause damage to business effectiveness or security • adversely affect parliamentary relations • impede the effective development or operation of SPCB policies and services • undermine the proper management of the SPCB and its operations • damage the reputation of the SPCB • lead to additional expenditure for or financial loss to the SPCB • work substantially against the SPCB's operational, contractual or commercial interests • breach a commitment to keep third party information confidential • breach statutory restrictions on the disclosure of information • compromise the confidentiality, integrity, or availability of SPCB data • undermine the privilege associated with legal advice • compromise the rights and freedoms of a living individual	Will cause **harm** – should be marked *Restricted.* *An appropriate descriptor should also be chosen to inform staff of the type of information being restricted.*	SP Online – apply the equivalent sensitivity label Outgoing email: apply the equivalent sensitivity label Other – apply the marking and descriptor clearly, for example in bold prominently on top of the page/file

Step 1	Step 2	Step 3
Harm test The compromise of information would likely:	**Select marking and descriptor**	**Apply marking and descriptor**
Confidential		
• place lives at risk • significantly undermine the safe and effective conduct of the Scottish Parliament • significantly undermine the decision-making process of senior staff • breach the commitment of the SPCB to secure employee personal information • significantly undermine the privilege associated with legal advice • divulge information which could be used to compromise the cyber-security of SPCB ICT systems	Will cause **serious harm** – should be marked *Confidential.* *An appropriate descriptor and group (where available) should also be chosen to inform staff of the type of information being restricted and which group it is restricted to.*	SP Online – apply the equivalent sensitivity label Outgoing emails: apply the equivalent sensitivity label Other – apply the marking and descriptor clearly, for example in bold prominently on top of the page/file. Take steps to ensure access to information is prevented to all unauthorised individuals.

Should the level of harm be considered more serious than the ***Confidential*** marking, staff should consult the Information Manager.

Appendix B – Handling marked information

Action	Not protectively marked	Restricted	Confidential
Application			
Marking electronic documents and records	No additional measures required from business-as-usual processes.	The Restricted marking sensitivity label should be added by the author of the document and prior to any distribution.	The Confidential marking sensitivity label should be added by the author of the document and prior to any distribution.
Marking email	No additional measures required from business-as-usual processes.	A Restricted sensitivity label should be added by the email sender.	A Confidential sensitivity label should be added by the email sender.
Marking hardcopy documents and records	No additional measures required from business-as-usual processes.	The protective marking, and descriptor if required, should be added by the information originator. Files containing hardcopy documents and records should have the marking applied to the file.	Same as *Restricted*
Changes			
Changing protective markings	Marking can be upgraded as required	Protective marking and descriptor can be upgraded to a Confidential marking or downgraded to *Not protectively* marked if required. Some information is time-sensitive, and it is therefore important to ensure that protective markings are amended when required. When changing the level of marking in SP Online a justification must be provided when prompted.	Protective marking and descriptor can be downgraded if required. When changing the level of marking in SP Online a justification must be provided when prompted.

Action	Not protectively marked	Restricted	Confidential
Storage			
Digital documents and records	Digital documents and records should be stored in SP Online.	Digital documents and records should be stored in SP Online where activities are audited.	Same as *Restricted*
Hardcopy documents and records storage	No additional measures required from business-as-usual processes.	Hardcopy documents or records should be physically protected by one barrier (e.g. a locked cabinet or pedestal). *Note: When protectively marked documents/records are added to a file/folder, that file/folder must immediately attract the same marking.*	Same as *Restricted*
Portable storage devices (PSDs)	No encryption required for PSDs containing information which is not protectively marked.	Restricted material should be stored on the Parliament's network or Cloud storage environment. If short-term storage on a PSD is required, the PSD should be encrypted. Unencrypted PSDs **should not** be used. Storage should comply with the *Information security policy*.	Same as *Restricted*
Removing information from SPCB premises and IT systems	Not protectively marked information can be removed from SPCB premises or IT systems to satisfy a business need.	Restricted information **should not** be taken off SPCB premises (or SPCB approved storage facilities) or IT systems and equipment without the permission of the appropriate office head. Protectively marked information assigned a *Personal* or *Staff* descriptor should not be removed from SPCB premises or IT systems regardless of office head approval. Should there be a need to remove Restricted information (that is not	Confidential information should not be taken off SPCB premises (or SPCB approved storage facilities) or IT systems and equipment

Action	Not protectively marked	Restricted	Confidential
		personal) from SPCB premises or IT systems, removal can be approved following completion of a risk assessment. Once removed, it should be carried in an appropriate container. The container should remain in the possession of the individual at all times and should not be left unattended in a public place. The information should not be entrusted to the custody of non-SPCB staff.	
Sharing			
Sharing – Internal (SPS)	Not protectively marked items should not be emailed as attachments – SP Online links should be used. No additional measures required from business-as-usual processes.	Email – Restricted items **should not** be emailed as attachments. SP Online links should be used. PSDs – PSDs **should not** be used to distribute protectively marked items to an internal audience. Hardcopies – Protectively marked items should only be sent through internal mail or delivered in person.	Same as *Restricted*
Sharing – MSPs	Documents should be emailed as attachments to MSPs' Parliament email accounts. No additional measures required from business-as-usual processes.	Email – Members do not have access to SPShare. Documents should therefore be emailed as attachments to MSPs' Parliament email accounts. The email subject should contain the protective marking that applies to the item. Restricted information should not be emailed to private email accounts.	Confidential information should not be shared with Members.

Action	Not protectively marked	Restricted	Confidential
		PSDs – PSDs **should not** be used to distribute protectively marked items to Members. Hardcopies – By post in a closed envelope. The envelope should not be marked with a protective marking or descriptor, other than PERSONAL or ADDRESSEE ONLY. It should be addressed to the Member by name.	
Sharing – External	No additional measures required from business-as-usual processes.	Restricted information must only be distributed externally to **authorised persons**. SharePoint – External SharePoint Sites (both SPS and third party) can be used to share Restricted information providing a sharing agreement is in place. Email – Restricted information **should not** be sent outwith the Parliament via email unless appropriate measures are taken to protect it. Appropriate measures include: • **Default transit encryption** - Transport Layer Security (TLS) to protect sent emails by default. • **Sharing agreement** signed by the recipient of the protectively marked information being shared on occasions where the sharing is more routine in nature. Prior to any agreement being signed confirmation of the recipient's	Confidential information should not be shared externally.

Action	Not protectively marked	Restricted	Confidential
		ability to support TLS encryption should be obtained. • **End-to-end encryption** - where additional steps are required e.g. when the information being shared is considered special category personal data, the protectively marked information should be protected with end-to-end encryption. PSDs – PSDs **should not** be used to distribute Restricted items to an external audience unless measures have been taken to protect items. Measures include ensuring the physical security of the PSD and encryption. Hardcopies – By post in a closed envelope. The envelope should not be marked with a Restricted marking or descriptor, other than PERSONAL or ADDRESSEE ONLY. It should be addressed to an individual by name.	
Request for information under information access legislation	N/A	Disclosure will be judged on a case by case basis. All information disclosed as a result of an information request e.g. FOISA, should have any protective marking removed.	Disclosure will be judged on a case by case basis. All information disclosed as a result of an information request e.g., FOISA, should have any protective marking removed.

Action	Not protectively marked	Restricted	Confidential
Disposition			
Destruction or transfer to NRS for permanent preservation	Normal disposition rules apply to unmarked information.	The Information Manager will seek the authorisation of the information owner prior to carrying out any disposition action.	As restricted.

Change log

The following table details changes made to this document.

Date	Reference	Details of change
30/08/2021	v1.0	Revised and updated system approved by the Chief Information Officer and Digital Workplace Programme Board (26/08/2012). Also endorsed by Leadership Group (30/08/2021).