UK Parliament

Parliamentary Protective Marking Scheme (PPMS)

Quick Reference Guide

Last updated October 2024

What is the Parliamentary Protective Marking Scheme?

The Parliamentary Protective Marking Scheme, or PPMS, is the House Administrations' policy which sets out how information of different sensitivity should be marked and handled. It helps users identify sensitive information and how to keep it secure.

Protective markings are added to information to inform users or recipients of the sensitivity of the material and identify the controls and handling measures needed to protect it from compromise.

There are four protective markings that should be applied to all parliamentary information, depending on its sensitivity.

The four markings are:

- Unrestricted
- Restricted
- Highly Restricted
- SECRET

Responsibilities

All parliamentary information has value and requires an appropriate degree of protection. Everyone who works with this information (including staff, contractors and suppliers) has a personal responsibility to safeguard and protect the information in their care.

By marking information, you are clearly stating the sensitivity of the information and reminding everyone of their obligations to keep it secure.

If parliamentary information is shared with you, it is important that you know how to handle it to keep it secure. The tables on the following pages summarise the handling requirements for each of the markings. These requirements apply whether the information was shared with you verbally, electronically, in paper format, or in any other way.

What you need to do

- Mark parliamentary information with an appropriate protective marking so that you and others know how to correctly handle and protect that information
- Handle information in a manner that is appropriate to the information's sensitivity.
- Only share sensitive information with others where there is a genuine 'need-to-know'.
- Report any suspected or actual compromise of sensitive parliamentary information in line with Parliament's information incident reporting processes.

An overview of the markings

Marking	Unrestricted	Restricted	Highly Restricted	SECRET
Definition	**Information which is not sensitive.**	**Information with some sensitivity.**	**Information that is particularly sensitive and carries high risk.**	**Parliament's most sensitive information.**
Harm if compromised	Would cause no harm or only negligible, short-term disruption or inconvenience.	Would likely cause inconvenience, delay or disruption, lead to loss of confidence, or minor reputational damage to a team or service.	Would likely cause significant disruption or damage to the workings of Parliament or endanger the security of individuals or the estate.	Would likely threaten life (an individual or group), seriously damage Parliament's security, UK national security and/or international relations, or seriously assist in the planning of or impede the investigation of crime.
Illustrative Examples	• Internal, non-sensitive policies and processes • Training and guidance materials • Floor plans displaying publicly known locations • Routine emails between staff • Team meeting notes and approved minutes • Press releases • Newsletters • Job descriptions	• Line management information • Budgets and other routine financial information • Legal advice on routine business matters • Business planning documentation • Recruitment candidate information • Tender documents • Draft reports and board papers on matters of some sensitivity • Draft business cases	• HR investigations • Contingency plans relating to systems failures • Medical referrals • Committee evidence of a highly sensitive nature • Floorplans revealing sensitive locations on the estate • Network design architecture • Legal advice on sensitive topics • Detailed preparations for a VIP visit	• Details of highly sensitive visit arrangements for individuals where there is a heightened threat profile • Detailed plans for sensitive security operations • Detailed security surveys, schematics and specifications which reveal vulnerabilities **Very few individuals or teams will handle SECRET information. This marking is therefore not covered in detail in this guide. Anyone receiving or creating information at this level will be briefed on the necessary security arrangements and handling requirements.**

Descriptors

- There are **9 descriptors** which can be used in combination with the markings **Restricted** and **Highly Restricted.**
- They describe the nature of the information and why the marking has been applied.
- If your information sits between two or more descriptors, align it to the marking that best describes the contents - only one descriptor can be applied to your information.

Commercial

such as procurement documents (for the period of commercial sensitivity).

Legally Privileged

such as formal legal advice.

Management

such as audit reports, business cases, or management planning.

Personal Data

such as medical referrals, line management reports and related information about an individual's employment.

Security

such as physical or technical e.g. risk and threat assessments and contingency plans.

Parliamentary Privilege

such as draft documents which will ultimately be sent to a Committee of either House.

Member Services

such as HR Advice for Members, travel bookings and library enquiry responses.

Parliamentary Commissioner for Standards

such as investigations carried out by the Parliamentary Commissioner for Standards.

For Committee use only

such as draft resports, final reports (prior to publication), informal notes from Committee meetings (draft) and briefings to the Chari.

Handling instructions

Activity	Unrestricted	Restricted	Highly Restricted
Meetings and discussions	• Can be discussed freely in public spaces. • Can be discussed in publicly accessible parts of the parliamentary estate. • Meeting attendees can brief back to their teams as they see fit.	• Avoid discussing in public or publicly accessible spaces. • Do not discuss if you can be overheard. • Use headsets and avoid repeating what others say out loud. • Meeting attendees can brief back to their teams but should check before sharing further.	• Do not discuss in public spaces • Use dedicated private meeting rooms or spaces. • Do not discuss if you can be overheard. • Use headsets and avoid repeating what others say out loud. • Meeting attendees can brief back to team members with a need-to-know.
Marking	Does not need to be marked.	**Hard copy information:** Display the marking in the header of the document and on the front cover of the paper file. **Digital documents and emails:** Include marking in document header and the subject line of emails.	
Sharing	• Can be shared with and accessed by all staff across Parliament. • Share using links, not attachments. • Always check the distribution list before emailing information.	• Obtain permission from the Information Asset Owner (IAO) before sharing. • Only share with named individuals on a need-to-know basis. • Share using links, not attachments. • Check the distribution list carefully before emailing. Avoid using bcc. • Recipients must have CTC clearance. If they do not, either do not share, or redact or remove sensitive elements before sharing. • Only share via approved methods. Do not send to freeware email accounts e.g. Gmail, Hotmail. • Ensure the information is protected during transit, e.g. by encryption.	
Moving / posting	• Use a single sealed opaque envelope/cover. Do not display the protective marking on the outer envelope/cover.	• Use double opaque envelope/cover. Do not display the protective marking on the outer envelope/cover. • Use a recorded mail service or an approved courier service. Include a return address.	

Handling instructions (continued)

Activity	Unrestricted	Restricted	Highly Restricted
Storage - digital	• Only store on corporately approved or accredited systems.	• Only store on parliamentary supplied or approved systems with appropriate technical controls applied to restrict access to those with a clear need-to-know. • Where storage on removable media is necessary, only use approved, encrypted media. • Do not sync to local devices. • Print only if necessary.	
Storage – hard copy	• Can be stored in unsecured offices and storage equipment.	• Store in an opaque folder and lock away when not in use and the room is unattended. • Avoid taking hard copy out of the office unless there is a clear business need.	
Consulting information	• Can be accessed in publicly accessible spaces.	• Operate a clear desk policy. Lock your screen (Windows key + L) when unattended. • Be aware of whether you can be overlooked by unauthorised individuals.	• Operate a clear desk policy. Lock your screen (Windows key + L) when unattended. • Do not access in publicly accessible spaces or where you can be overlooked. • Risk assess before accessing in high-traffic areas, such as canteens or 'drop in' workspaces.
Destruction – hard copy	• Can be disposed of in recycling or general waste.	• Do not dispose in standard recycling or general waste. • Securely destroy in a way that prevents recovery or unauthorised access.	
Destruction - digital	• Delete through an auditable process which makes the data irrecoverable.		

Remember

- All parliamentary information has value and requires an appropriate degree of protection.

- Everyone who works with this information (including staff, contractors and suppliers) has a personal responsibility to safeguard and protect the information in their care.

- By marking information, you are clearly stating the sensitivity of the information and reminding everyone of their obligations to keep it secure

- You should not assume that information which is **unmarked** or marked **Unrestricted** is always correct - sensitivities may have been missed at the point of creation or through the evolution of the drafting process or email chain. Users should always check the marking of information they create or receive to ensure the right marking has been applied, and check or challenge if unsure.

- The sensitivity of information may change over time. Protective markings should be **regularly reviewed and updated** where needed.

- Application of the scheme does not prevent disclosure under FOI.