HOUSE OF LORDS

Management Board

Information Security Update

Responsible Board Member(s)	Rhodri Walters
Paper prepared by	Rhodri Walters Alex Daybank; Information Compliance Manager
Date	17 May 2010
Summary of actions requested:	The Board is asked to agree the introduction of the Protective Marking Scheme (summarised in the annex to this paper) for sensitive information held by the House of Lords administration.

Introduction

1. The Board will be aware that a protective marking scheme has been used across government for many years. Information assurance audits of each House recommended the introduction of such a scheme for use by Parliament. A scheme will further ensure that sensitive information is recognised and handled as such. The need for the scheme to be bicameral is widely accepted due to the fact that use of it should become part of the routine records management processes of each House and these are already conducted on a bicameral basis.

The Parliamentary Protective Marking Scheme

2. The Board will wish to note that the proposed version it is now being asked to agree has been agreed by the House of Commons Management Board in March, subject to consultation and agreement by the House of Lords administration. Consultation with the administration was conducted by the Information Compliance Manager and the Information Security Co-ordinators in each office.
3. Extensive work has been carried out across each House to produce a workable scheme which can be adopted with minimum disruption to existing working practices. (The final version of the suggested Parliamentary scheme is attached at Annex 1.) The Board will see that the suggested version differs from that of the government scheme in that it contains only one category of protective marking.
4. Consultation across each House found that most sensitive information handled by staff is not sufficiently sensitive to require use of a scheme with multiple levels and that sensitive Parliamentary information roughly equates to the 'Restricted' level in the government scheme.
5. Separate procedures will continue to apply to information received from government which carries a marking of 'Confidential' or above.

The Committee Offices

6. Following consultation, the Committee Offices of each House have decided to opt out of the proposed scheme for committee papers while agreeing to its adoption for other sensitive information created by each office such as staff appraisals. This decision resulted from a general consensus within both offices that they would be unable to mandate Members to observe the handling requirements connected to the use of the Protective Marking Scheme.

7. The House of Commons Management Board has agreed to the continued use by their Committee Office of their own 'Document Security Scheme.' The House of Lords Committee Office has stated that, subject to approval by the Board, it will now add its own marking to all papers which are the property of the Committee to ensure Members and staff of the administration are aware there may be sensitivities attached to the information. They have also stated that where appropriate they will ensure these papers are handled in a manner compatible with the requirements contained within the Protective Marking Scheme.

17 May 2010 **Rhodri Walters**

Overview of Parliamentary Protective Marking Scheme

For further information refer to detailed guidance

ASSESS THE HARM AND DECIDE WHETHER IT IS APPROPRIATE TO MARK THE INFORMATION 'RESTRICTED ACCESS'

- **The creator of the information decides whether a marking should be applied using the criteria at step 1 below**
- **Only apply a marking after considering this harm test. If you are unsure, you should consult your manager**

Use of a protective marking will not prevent its disclosure under the Freedom of Information Act; a marking will however alert those making decisions regarding its disclosure to any sensitivity which might apply. Requests for information will continue to be considered on a case by case basis by each House.

STEP 1: APPLY THE HARM TEST. Questions to ask:	**STEP 2: SELECT APPROPRIATE DESCRIPTOR**
If the information was lost, stolen or disclosed without authorisation, would it:	**Indicate why the marking has been applied** To indicate the nature of the information's sensitivity.
• Affect service delivery to Members or otherwise impact on general operations • Endanger individuals, Parliamentary assets, property or the physical security of the Parliamentary Estate • Endanger critical business or communication systems • Risk a breach of statutory obligations (including data protection) • Cause financial loss to the House, the public or to those with whom we otherwise conduct our business • Assist the planning of a crime or impede investigations Or otherwise give rise to a risk that the work of either House would be obstructed or impeded.	**COMMERCIAL** – considered or accepted tenders; other procurement documents **LEGAL -** formal legal advice **MANAGEMENT -** audit reports**;** business cases; the exchange of advice; management planning **PERSONAL DATA** - medical referrals, reports and related information; information about an individual's employment; material only to be seen by the person to whom it is addressed **PRIVILEGE*** - e.g. advice to Members on proceedings which are of a sensitive nature **MEMBER SERVICES HoC only-** e.g. DIS Enquiries database, allowances, special address list, PAS advice **SECURITY** – physical or technical e.g. business continuity or disaster plans; security policies, ICT network schematics

* Parliamentary Privilege will not in itself mean a document will necessarily require additional protection, the sensitivity of the privileged information were it to be lost or inappropriately disclosed must be considered e.g. privileged information which is produced for almost immediate publication is unlikely to require protection and therefore a marking.

On rare occasions the risk of harm might be considered so severe that additional security measures may be warranted – in these circumstances advice must be sought from the SIRO(Senior Information Risk Owner)routed through the DIRO (Departmental Information Risk Owner) for HoC, Information Compliance Manager for HoL.

If the document carries an externally assigned security marking

Handle the information in accordance with the controls set by that body; e.g. HM Government Protective Marking Scheme *[Further information included in the detailed guidance]*

OR If the information relates to a committee

Committee papers, including draft reports, relating to the committees of each House will be dealt with under alternative document security schemes.

Please refer to the detailed guidance for complete information.

Overview of Parliamentary Protective Marking Scheme

For further information refer to detailed guidance

Applying the marking and descriptor	**Document:** Apply the marking and descriptor in BOLD CAPITALS, centred at the top of the document (in the header field on each page of documents with multiple pages). **File:** Apply the marking on the front cover **Emails:** Apply marking and descriptor in the subject line of email e.g. **RESTRICTED ACCESS - COMMERCIAL**
Storing paper documents and files	Physically protect by one barrier (e.g. a locked cabinet or pedestal) within the Parliamentary Estate or when working remotely. (This includes information identified for disposal).
Storing of data on IT systems	Permitted on the Parliamentary Network, in accordance with IT security policies and procedures. Ensure access rules are applied; i.e. administration rights and user permissions to restrict access to folders as appropriate.
HOWEVER YOU TRANSMIT INFORMATION, WHETHER MARKED OR NOT, YOU SHOULD ONLY SHARE IT WITH SOMEONE WHO HAS A BUSINESS NEED TO SEE IT	
Distributing hard copy documents internally	Permitted. Use internal mail or deliver in person. Mark the envelope. Do not just use an internal transit envelope.
Distributing hard copy documents externally	Permitted. Double envelope with return address. Do not show protective marking on the outer envelope.
Email within Parliamentary network	Permitted. Show marking and descriptor on subject line. Consider using password protection for attachments. Consider whether other users have access to recipient's e-mails – see detailed guidance for further information.
Email to non Parliamentary accounts - including government departments	Only if necessary, but with caution. Password protect attachments. Show marking and descriptor on subject line. Do not include sensitive information in the email itself. Do not e-mail this information to personal e-mail accounts such as hotmail. Seek agreement from your line manager first.
Using portable media; e.g. memory sticks, laptops	Only encrypted devices should be used to store or transport such data.
Using the phone (landline, mobex or mobile)	Only if necessary, and with caution, particularly if away from the office. Confirm who you are speaking to and keep discussion of protected detail to a minimum.
Faxing	With caution. Ensure recipient is ready to receive information and also have them confirm receipt.
Photocopying	Permitted but limit distribution and dispose of excess copies securely.
Removing from the Parliamentary Estate	Permitted, but must be with line manager's permission. If electronic information use encrypted PICT supplied ICT, such as laptops and encrypted memory sticks. See detailed guidance.
Disposing of papers	Use confidential waste bins, sacks or shredders where available. Particularly sensitive information should be shredded.
Re-using or disposing of memory sticks and other portable devices	Delete contents and re-use within Parliamentary Estate only. Contact PICT for secure destruction.