

HOW DO I...HANDLE AND DISPOSE OF INFORMATION?

Vetting requirements for all staff and contractors:

The Baseline Personnel Security Standard (BPSS) is applied to all staff, contractors, secondees, placements etc. Those who may need access to more sensitive information may also need to be vetted to Counter Terrorist Check (CTC) level. For further information visit our [security vetting](#) intranet page.

Handling / storing information:

Sharing Information

- When sharing information outside the Welsh Government care must be taken to secure the information from inadvertent/malicious loss or corruption.
- For further information see [How do I ... Share Hard Copy Information Securely](#) and [How do I ... Share Electronic Information Securely](#).

Protective Markings

- OFFICIAL-SENSITIVE information must be clearly marked but there is no need to include the OFFICIAL marking on documents or emails.
- The protective marking must appear at the top and bottom of each page of each document. Any special handling instructions (e.g. do not print the document) must be outlined at the beginning of the document. When emailing information the protective marking must appear at the beginning of the email along with any special handling instructions. For further information see [How do I ... Use Government Security Classifications](#).
- For OFFICIAL-SENSITIVE information take additional precautions such as numbering pages in a way that makes it easy to spot if any are missing e.g. '1 of 6'
- OFFICIAL-SENSITIVE information (hardcopy or removable media) must not be removed from the office without prior authorisation from your Information Asset Owner / Deputy Director (IAO).
- If new information on an OFFICIAL file (hardcopy or electronic) makes it more sensitive it must be re-classified as OFFICIAL-SENSITIVE. Only the owner of a document/file can down-grade its classification.

Storing Information

- Store information only on iShare (or other approved document management system e.g. CMS). Access must be authorised on a 'need to know' basis.
- Control copy documents, reviewing spare copies regularly and destroying them if not required.
- Lock away physical files/removable media when not in use. Adhere to the [Clean Workspace Policy](#) and lock computer screens when leaving your desk.
- Information, laptops and mobile devices (e.g. Smartphones) must be stored in a secure location overnight and not left unattended when working outside the office or travelling.

Disposing of information:

Dispose of sensitive paper waste by shredding (using a shredder provided by the Welsh Government) or through an approved secure disposal contract. Information on removable media should be disposed of via the ICT Disposals Contract through a MyIT Service Request.