

**Policy Statement on Data Security and Use of IT Equipment By
Contractors/Consultants and Agency Staff Employed By The Ministry of Justice**

Contractors, consultants and agency staff providing services to MoJ may use their own computing facilities to deliver those services with the following conditions:

1. These computing facilities must be their 'tools of trade', i.e separate from personal computing facilities used by themselves or their families etc. for leisure or other personal uses; and must employ best practice security controls such as up to date anti-virus control, personal firewall, access control, disk encryption and up to date software patches.
2. Use of these computing facilities should be limited to activities involving MoJ data such as producing reports, reviewing documents, sending and receiving emails, and should not involve storing and processing large volumes of MoJ data, for example database extracts.
3. The disk encryption employed must conform to the FIPS140-2 standard or CAPS (CESG Assisted Product Scheme).
4. If the data warrants a RESTRICTED marking the disk encryption employed must conform to CAPS except in exceptional circumstances e.g. short timescales, lack of alternative product etc., where a FIPS140-2 certified product may be employed as a short term, interim measure. In this instance, senior management approval must be obtained and documented in an email to the Information Assurance email account. If long term access to RESTRICTED data is required MoJ computing facilities must be provided.
5. Where the computer connects to a remote network e.g. the contractor's company network, then an encrypted link must be used.
6. No emails containing protectively marked or personal data should be sent un-encrypted over the Internet. Personal and protectively marked emails, up to RESTRICTED, may be exchanged via the Criminal Justice Secure Mail System (CJSM). The CJSM is accredited to handle RESTRICTED - Criminal data, so consideration should be given to the suitability of CJSM where the data relates to other types of RESTRICTED information e.g. Policy. Guidance on determining what is personal data is available from the Information Commissioner's Office (ICO) website at www.ico.gov.uk.
7. Any removable media used to transport data outside of secure buildings must be encrypted with a product certified to FIPS 140-2. Once no longer required these devices should be securely disposed of. CD/DVDs and floppy disks should be cut into 4 pieces and disposed of as normal waste.
8. Computer hard disk drives should be securely erased before disposal or recycling if it has held any personal or protectively marked data. Information Assurance Branch should be consulted on the procedure to be followed.
9. In compliance with the Data Protection Act, any personal data must be deleted when no longer required, thus must not be retained beyond the duration of engagement with the MoJ.
10. Where there is a need to provide access to large volumes of personal or protectively marked data only MoJ computing facilities must be used. Removable media provided by MoJ must be returned to the MoJ after use.
11. Paper records containing personal data should be stored, transported and disposed of securely. Sensitive waste paper should be collected separately from normal waste, and stored securely pending destruction by shredding or burning. As with electronic records, particular care should be taken when moving bulk paper records.