1. Types of information requiring confidential disposal

Personal Information (personal data)

The DPA defines personal data as any information that relates to an identifiable living individual (the data subject) who can be identified from that data or from other information in the possession of, or likely to come into the possession of, the data controller. Thus, any document containing personal information of students, staff or any other living individual must be disposed of confidentially. If unsure as to whether information constitutes personal data it is always preferable to err on the side of caution and opt for confidential disposal.

Sensitive Personal Information (sensitive personal data)

The DPA makes separate provision for personal information classed as sensitive personal data. Personal data will be regarded as sensitive where it relates to:

- Ethnic or racial origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sexual life
- Criminal offences or alleged criminal offences

Records relating to internal disciplinary or grievance related matters of staff and students are also considered sensitive personal information.

This type of data is subject to further constraints on processing and requires a greater level of security in its storage, handling and disposal.

Business Sensitive Information

In order to protect its own interests as a corporate body, the interests of bodies it deals with and to avoid legal action for breach of confidence the University needs to ensure that documents and records which contain business sensitive information are confidentially destroyed. Such information may include:

- Confidential financial activities
- Unpublished information relating to future planning, policy and strategy development activities
- Intellectual Property related information, such as unpublished research data, draft research papers, manuscripts and dissertations
- Legal documents
- Confidential information in contracts and tenders
- Confidential information received from suppliers and customers.
- Information likely to prejudice the commercial interests and activities of the University

With the exception of clear cut confidential information such as legal documents and contractual information, it is not possible to be absolute as to what constitutes business sensitive information, as the sensitivity of information often changes according to context and time. Therefore a degree of individual judgement and discretion is required in identifying
business sensitive information which needs to be securely destroyed. Guidance from senior management responsible for the area of work to which the information relates should be sought.

However, the costs incurred by the University in confidentially destroying its paper waste through the confidential waste disposal bags are significant, so if the information is not genuinely business sensitive it should go in ordinary waste recycling sacks. As a general rule, non-personal information which has no apparent business sensitivity and/or is made readily available or published by the University should be disposed of in non-confidential sacks.


Cross Cut Shredding

Shredding of documents and records in the office using a high security cross cut shredder should be undertaken in respect of:

- Sensitive personal information
- Highly business sensitive information

The shreddings can be disposed of in ordinary paper waste recycling sacks.

Confidential Paper Waste Disposal Sacks

Disposal of documents and records in confidential paper waste disposal sacks, which are collected and taken off site for shredding, should be undertaken in respect of:

- Non-sensitive personal information
- Business sensitive information

3. Disposal of Electronic Documents and Records

Information held on network storage can be considered to be securely disposed of once deleted.

To ensure confidential destruction of personal and business sensitive information stored on magnetic storage media (including computer hard discs) degaussing will be necessary to permanently erase the data. Physical destruction of the storage disc (i.e. through a shredder or cutting up) will be required for information stored on optical media.

Data Protection Unit
Data.protection@stir.ac.uk

Updated January 2015