Information classification guidelines

Background

The University's Information Security Policy identifies two categories of information: **open** and **restricted**. As with everything in the policy the format of the information is not important: classification applies equally to information in hard copy and digital formats.

Open information
Information that is open may be freely shared, inside and outside of the University.

Restricted information
Information that is restricted may be shared under some circumstances, including in response to Freedom of Information requests, but the key is that thought and consideration should always be given first to how the information is shared, with whom it is shared and why it is shared. Steps should always be taken to ensure that the information is not accidentally shared with anyone who does not have a need or a right to see it.

Some information may start open and become restricted, such as a blank template, form or spreadsheet which will only become restricted once it is filled in. Other information will start as restricted and become open over time, such as plans to open a new department or create a new course.

The University's Information Security Policy requires extra protection for restricted information in all areas. Some areas hold high levels of restricted information and they have additional requirements which are laid out in a separate document. Those additional requirements may include a more granular approach to information classification.

Responsibilities

The main purpose of some information being restricted is to encourage those who handle it to stop and think. It will often be obvious from the content and the context whether or not information, data or documents can be shared. Where it is not obvious then advice must be sought.

The Head of Section or Department must ensure that restricted information in their area is properly identified and protected accordingly, particularly where an entire system holds restricted information.

Data Champions will support the Head and staff through ensuring that everyone knows how to identify and protect restricted information, ensuring colleagues are aware of relevant polices and have access to training and advice.

System owners must ensure that there is adequate access management in place, and that any incidents are followed up and investigated as soon as possible, following any relevant reporting protocols.

Individuals who are producing information, data or documents must take steps to ensure that recipients understand why they are being given the information and what restrictions there are on it use.

Individuals who access information must ensure that they handle information that is restricted in accordance with the University's Information Security Policy and other applicable policies and guidelines. They must seek advice if they are not sure of the classification level of a particular type information.

Marking restricted information

Wherever possible information that is restricted should be clearly marked as such. There are no set ways of doing this – much will depend on the format in which the information is shared and the method of sharing. Document watermarks, headers or footers, title pages or cover sheets would all be possible. If electronic items might also be printed then the marking must be in a form that will appear in the printed version.

Marking should be immediately obvious, not buried in a document. If circulation is to be limited to a specific group or a specific time period, then that should be made clear.

Restricted information should also always include the name of the person or office that has created the copy or that owns the originating data set.

Restrictions might mean that the information is only for use within a particular group of people, e.g. a working group, committee, or department. It may mean that the information can only be used by staff, or it may only be shared within the University.

Research Data

Sharing data for scrutiny and reuse is an important part of research and can often be a prerequisite for receiving research funding. Where possible data will be open at the point at which the research is published, but up to that point it may need to be restricted. Personal data about research participants may need to be redacted, pseudonymised or anonymised before it can be shared. It is best practice for research data management plans to identify data or information that will need to be restricted, the groups or individuals to whom access is restricted, and the time period for which the restriction is valid. Note should also be taken of the Research Data Management Policy.

Help and advice

Advice may be sought from the relevant Data Champion or from the Information Assurance Manager.

Where there is any doubt the default must always be to treat material as restricted until it is confirmed to be otherwise.

Appendix A - Examples of restricted information

The following types of information will be restricted. This is not an exhaustive list.

- Personal information (information about identifiable individuals), in particular, information about racial or ethnic origin, sexuality, religion beliefs, trade union membership, physical and mental health, sexual life and criminal record
- HR files including Occupational Health files
- Individuals' payroll details, including bank details
- Student files including counselling files and conduct files
- Intellectual property, trade secrets, commercially confidential information, information provided in confidence, non-disclosure agreements
- Legal advice
- Reserved committee business, closed sessions of committees
- Information about the University's plans for the future, including recruitment targets, intention to buy or sell land, the opening or closure of departments, programmes or courses, staff redundancies or significant restructuring.

- Negotiations with third parties including academic partners, trade unions, contractors, business partners

Sara Stock
Information Assurance Manager

Approved by ICT SG: 18 November 2016

V1.0	Draft for discussion	05/07/2016
V1.1	Updated to include groups that restriction might cover and responsibilities of those producing information	25/08/2016
V1.2	Updated following input from Director of IT Services – document marking, research data – moved examples to an appendix	30/08/2016
V1.3	Inserted reference to research data management policy	10/10/2016
V2.0	Approved by ICT SG – final version for publication	18/11/2016