Ulster University Standard Cover Sheet

Document Title	PROTECTIVE MARKING STANDARD 2.5
Custodian	Deputy Director of Finance and Information Services (Information Services)
Approving Committee	ISD Committee
Policy approved date	2017 – 09 – 08
Policy effective from date	2017 – 09 – 08
Policy review date	2018 – 09 – 08

Changes to previous version

INTRODUCTION AND BACKGROUND

This document describes the three levels within the University Protective Marking Scheme and offers examples of how Protective Marking might be applied to various documents. Implementation will be aided by staff training and development and through complimentary policies, standards and guidelines.

The scheme provides the rationale for various management controls which External and Internal Auditors have recommended to be introduced and might represent guidance to staff in their handling of Personal[1] and Sensitive[2] information, and also materials shared with third parties and subject to contractual or other controls. The following audit observations apply in respect of control of University information and the use of technologies to support that control. Principle 7 of the Data Protection Act, (1998) requires that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data[3]."

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;

[1] As defined by the Data Protection Act 1998: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

[2] As defined by the Data Protection Act 1998: the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union , his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

[3]An extract from the Information Commissioner's website https://ico.org.uk/. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to: design and organize your security to fit the nature of the personal data you hold and the harm that may result from a security breach; be clear about who in your organization is responsible for ensuring information security; make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and be ready to respond to any breach of security swiftly and effectively.

- Freedom of Information Act 2000;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

STANDARD

Three-level System

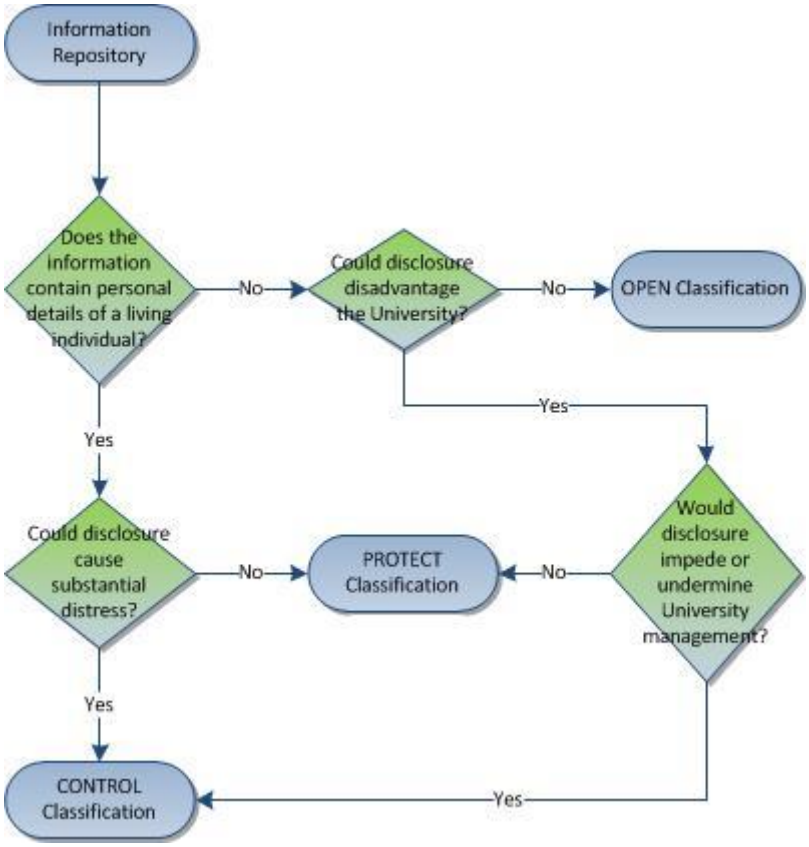
The University shall have a three-level system for the protective marking of records:

Marking	The rationale for selection	Example Document
OPEN	Unmarked material is considered open or unclassified. The term "OPEN" may be used to explicitly indicate that this is the case.	Most of the University's correspondence, administrative correspondence and Teaching & Learning materials. Copyright continues to be protected.
PROTECT	These documents if compromised could: • cause distress to individuals • breach proper undertakings to maintain the confidence of information provided by third parties • breach statutory restrictions on the disclosure of information • cause financial loss, loss of earning potential or could facilitate improper gain or advantage for individuals or companies • prejudice the investigation or facilitate the commission of crime • disadvantage the University in commercial or policy negotiations with others.	Personnel Records Completed Staff Appraisals Health Records Student Records Banking and Credit Card Details Pre-contract papers and opinions. Exam papers prior to the examination. ACCESS NI Reports PSNI Reports about ill-discipline Disclosures under The Rehabilitation of Offenders Act (1974)

		Disclosures of Sex Offender Register Entries. System passwords and other controls on access to Enterprise-level systems
CONTROL	Additional to those points included in the "PROTECT" classification, these documents, if compromised could: • cause <u>substantial</u> distress to individuals • make it more difficult to maintain operational effectiveness • impede the effective development or operation of University policies • undermine the proper management of the University and its operations.	Information shared subject to written description of the access arrangements, controls and permissions. Information gathered for the purposes of disciplinary proceedings. Mammograms and all other clinical records and notes shared with the University. Commercially sensitive information released "in confidence" Planning data. Complete "views" of a database of individual reports and entries – a full view of a class or cohort's exam results.

Protectively marked material shall be marked in UPPERCASE LETTERS, and shall be marked clearly in the document header and footer or where inappropriate to use header & footer, by means of a watermark.

The following diagram illustrates in the simplest terms, the general and most common quick "rule of thumb" decisions for classification in the most common cases.



IMPLEMENTATION

This Standard will be incorporated into training and information materials and will, where appropriate, inform technical and engineering decisions such as the necessity to encrypt portable devices such as laptop computers, portable storage and other portable devices (like smartphones), and the additional protection required for on-line systems and services. Where administration or academic endeavour require that personal, sensitive or clinical data is aggregated, this standard provides the basis for risk assessment on the storage and transmission of such University information.

Portability of Information

Information gathered by the University on business systems will retain the Protective Marking of the system from which it is extracted when transferred to another format or document. Portability of information creates particular issues which need to be addressed with the information custodian - particular attention must be paid to safeguard against the risks presented by “secondary processing;” the use of information for purposes other than those for which it was volunteered.

Discipline

Where necessary, this standard assists with the definition of the damage, or potential damage, which the University may be exposed to through the inappropriate handling,

extraction or deletion of information. As such, it informs the staff and student disciplinary systems.

Disclosure

Information, documents and the content of University systems may still be the subject of disclosure requests under court and tribunal orders, the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004. Internal protective markings are not a defence against responding to such requests. The University is obligated to respond to requests for information irrespective of where or in what format it is stored. Exemptions may be claimed in respect of each of the legislation and in accordance with the provisions of the legislation. For example, an HR record or entry might be subject to a disclosure request by a member of staff irrespective of the fact that it is marked PROTECT-PERSONAL. Unless an exemption can be successfully applied, the information will have to be provided.

Storage

Storage or transmission of sensitively classified information to locations outside the European Economic Area (EEA) risks placing the University in breach of its statutory responsibilities to safeguard information.