Information Classification Policy

Version:	**2**
Dated:	**01 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
V 1.0	May 2018	D. Waymouth	Original policy
V 1.1	May 2018	R. Cockram	2018 Update Revision
V 2	May 2018	R Platt	Approved Version

Approval

Version	Approval Board	Date of Approval
V 2.0	Information Governance & Security Steering Group	May 2018
V1.0	ISSG	June 2014

Contents

1.0 Introduction

1.1 The University generates and holds a wide variety of information that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of such assets is also necessary to comply with legal and regulatory obligations such as relevant Data Protection legislation, and to ensure efficient handling of Freedom of Information requests. Different types of information require different protection measures and therefore, applying classification markings of information assets is vital to ensuring effective information security and management.

2.0 Purpose

2.1 This Information Classification Policy together with the accompanying technical marking controls are intended to help staff and students determine what information can be disclosed to external parties, as well as the relative sensitivity of information that should not be disclosed outside of the University of Exeter without proper authorisation.

2.2 This policy also helps all members of the University to ensure that correct classification and handling methods are applied to their day to day activities and managed accordingly.

2.3 University information assets should only be made available to all those who have a legitimate need to access them.

2.4 The integrity of information must be maintained; information must be accurate, complete, timely and consistent with other related information and events.

3.0 Scope

3.1 This policy guidance covers information that is either stored or shared via any means including those created prior to the publishing of this policy. This includes: electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing).

3.2 Where the University holds information on behalf of another organisation with its own classification system, an agreement shall be reached as to which set of technical controls and handling guidelines shall apply.

4.0 Definitions

Data Management Plan:	A Data Management Plan (DMP) outlines what and how data will be created or collected and how it will be shared and preserved. A DMP also outlines your plans for sharing and preserving data in the longer-term. A DMP can be adapted as a project advances and it should be reviewed regularly as your data needs change
Data Protection Impact Assessments (DPIA):	A method of identifying and addressing privacy risks in compliance with GDPR requirements.
Freedom of Information:	Information held by the University may be requested under the Freedom of Information act and subject to exemptions will be disclosed. This classification scheme will help identify information where there may be exemptions that can be applied to allow the University to withhold information. Information which has been classified as internal or possibly restricted/confidential may still be subject to requests and potentially disclosable, the classification scheme is a useful indicator but does not

	provide a guarantee that information will not be disclosed, each request will be considered on its merits.
Information Administrator:	An individual who is responsible for the maintenance and protection of the information.
Information Asset:	A body of information which is organised and managed as a single entity and value for the University
Information Asset Owner:	An individual who has final responsibility of data protection and would be held liable for any negligence when it comes to protecting the University's information assets. This person may be a senior executive in the management team, head of a specific department or a professor in the case of research.

5.0 Responsibilities

5.1 The Information Governance and Security Steering Group is responsible for:

- Approving the Information Classification system, associated data management policies and any subsequent changes to these and
- Publicising the classification system and data management policies for electronically stored information.

5.2 Exeter IT will:

- Provide appropriate IT facilities/mechanisms to facilitate compliance with this policy for centrally maintained information.

5.3 Information Asset Owners and Information Administrators are responsible for:

- Identifying the appropriate information classification level for any information within their care
- Ensuring that the appropriate management policies about storage, publishing, disposal etc. are followed. Where information is classified not for public consumption (i.e. Internal, Restricted or Confidential) this should be clearly articulated to those who have access to such information.
- Ensuring that information is processed and managed in accordance with the University's Information Governance and Security Policies.

5.4 All members of the University (including staff, students, contractors, agency workers and associates) are responsible for

- Handling information in accordance to their classification
- Complying with this policy and with relevant legislation.

6.0 Policy

6 . 1 There are 4 levels of classification (Examples in Annex A)

Confidential	Available only to specified and relevant members, with appropriate authorisation. A breach of confidentiality could result in unacceptable damage with very serious and lasting consequences threatening the University or one of its activities.
Restricted	Available only to specified and / or relevant members, with appropriate authorisation. A breach of confidentiality could cause serious damage resulting in the compromise of activity within University in the short to medium term. This includes both personnel data and research data.
Internal	Available to any authenticated member of the University. Typically, if this level of information was leaked outside of the University, it could be inappropriate or ill-timed.
Public	Available to any member of the public without restriction. This information however should not be placed into the public domain without reason, such as a request or publishing as part of data management policy.

6 . 2 It is possible that we could receive information that is classified by Government or other institutions as Secret. Information classified as Secret will only be generated by the University incredibly rarely. It is reserved for information that could impact on National Security, potentially destabilizing the UK or its allies, including information which is subject to the Official Secrets Act 1989. The information handling requirements associated with this level will be dictated by the Information Asset Owner on each occasion. Where information of this level is processed additional security may also be provided.

6 . 3 All information held by or on behalf of the University will be categorised according to the Information Classification level (6.1 above).

6 . 4 The Information Asset Owner will assess the value, sensitivity and the risk of confidentiality breach to their data set. Once the classification has been established any documents containing this information must be systematically marked as such. Information Asset Owners will be identified by departments and recorded with the information assets on the University's Information Asset Register. It is recommended that data sets are larger rather than smaller to limit administrative complexity and overhead.

6 . 5 Any information which is not explicitly classified will be classified as confidential, pending classification, by default to avoid data leakage. In the case of disagreement over the classification level to be used, the more secure level should be adopted. Questions about the proper classification of a specific piece of information or a dataset should be addressed to your manager. Where there is a mix of information from different classification levels, the more secure level should be adopted. (Example in Annex B)

6 . 6 All information must be secured to meet the requirements of their respective classification levels (6.1 above). Guidance on the type of security controls that should be implemented is available in the Information Handling Guidelines.

6 . 7 Where a third party will be responsible for handling the information on behalf of the University, the third party shall be required by contract to adhere to this policy prior to the sharing of information.

6 . 8 Where information is discovered to have been incorrectly classified, or not to have been managed in accordance with its Information Classification, this should be reported immediately to the IT Helpdesk who

will log the incident and refer it to the appropriate team, information administrator or Information Asset Owner as appropriate for them to action.

6 . 9 All IT projects and services which require significant handling of information should have a DPIA indicating the information assigned to each classification level and the data management controls to be applied. The DPIA should be made available on request to the Information Governance Department and those authorised by the University to carry out security audits.

It is good practice to compile a data management plan for Research Project, even if you are not required to do so by your funder, especially if you are working in collaboration with others. A DMP can be adapted as a project advances and it should be reviewed regularly as your information needs change.

7.0 Contacts

Any queries or proposed amendments should be referred to the Information Governance Office at dataprotection@exeter.ac.uk.

Annex A: Example Information Classification Levels

Confidential

i. Highly sensitive data that will explicitly identify individuals which, if disclosed, puts the individual at risk from identity theft, social or legal sanctions, targeting by marketing corporations or pressure groups, threats from criminal or vigilante individuals or organisations
ii. Any data which is classified as special category data under the GDPR. For more information on GDPR within the University please visit: http://www.exeter.ac.uk/gdpr/.
iii. Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees).
iv. Draft research reports of controversial and / or financially significant subjects
v. Preliminary degree classification or transcript information pending formal approval and any publication
vi. Passwords
vii. Future marketing or student fees information not yet agreed to be made public.
viii. Legal advice and other information relating to legal action against or by the University.

Restricted

i. Business-sensitive data such as detailed financial records, information on commercial contracts.
ii. Personal data identified under the Data Protection Act 1998 (or its successor legislation). For more information on GDPR within the University please visit: http://www.exeter.ac.uk/gdpr/.
iii. Research data with intellectual property implications
iv. Internal correspondence, timesheets, expenses.
v. Exam scripts, exam marks, examiner's comments on a student's performance
vi. Incomplete reports and other documents whose integrity may be damaged by uncontrolled/unauthorised changes, or whose leakage may cause damage to the project, the project funders or the Institute

Internal

i. General University data: all staff internal memoranda
ii. University policy and procedures
iii. Data that is already in the public domain but was not intended as such and could result in litigation if republished.
iv. Staff directory including email addresses.

Public

i. Public data will have no significant impact if they are altered or viewed in an uncontrolled fashion.
ii. Principal University contacts e.g. name/email address/telephone numbers for public-facing roles will be made freely available
iii. Annual Accounts
iv. Pay scales
v. Program and course information

Please note that the volume of data may result in a high classification level and/or more secure data handling methods.

Annex B: Example Mixed Information Classification Levels

If a database were to store student welfare information (confidential) alongside course programme details (internal) the whole data set would be classified as confidential.

Where a subset of information is extracted from a highly classified set of information, the information classification level should be reassessed.

If the programme details were extracted from the above database and stored in a spreadsheet for an annual review and update, this spreadsheet should be handled as internal information, not confidential.

Annex C: Data Management Plan contents

Information about research data management plans can be found in the Research Toolkit:

http://www.exeter.ac.uk/research/toolkit/developing/writing/dmp/

Further queries regarding data management plans should be directed to the Library via rdm@exeter.ac.uk.