Data Classification Policy

1 Introduction

UCD's administrative information is an important asset and resource. All administrative information is categorised according to appropriate needs for protection, handling and compliance with regulatory requirements.

The purpose of classification is to ensure that information is managed in a manner appropriate to the risks associated with ensuring that it remains reliable, trustworthy and available for appropriate use.

2 Application of Policy

2.1 All **Information Owners** are responsible for ensuring that this policy is adopted within their area of responsibility.

2.2 The classification of information will be the responsibility of the **Information owner**; e.g. financial data to the Bursar; staff data to the Head of HR.

2.3 **Individual staff members** are responsible for ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification.

3 Policy Statement

3.1 All existing administrative data belongs to one of the classifications in section 5.

3.2 Where data is not classified according to another category, it is to be handled as per the requirements for controlled data.

3.3 All new information assets categorised as confidential or higher should be categorised & labelled for handling according data handling procedures defined by the **Information Owner**.

3.4 Controls must be implemented by the **Information Owner** according to the classification to which the data belongs.

3.5 Data is classified, and may be reclassified, by the **Information Owner**.

Note: Categorising information does not exclude it from consideration for disclosure under Freedom of Information or Data Protection legislation.

4 Further Information

4.1 Any queries relating to this policy should be directed to the Information Security Officer, UCD.

5 Data Classification Guide

This guide provides a framework for classifying and protecting UCD's information resources. It outlines the area of risk in the left column and the adjacent cells show the possible impact of unwanted/unauthorised disclosure or alteration for each classification.

Reason for Classification	Strictly Confidential	Confidential	Controlled
Legal Requirement	Protection of data is required by law or regulatory instrument.	UCD has an obligation to protect the data	Protection of data is at the discretion of the owner or custodian
Examples	*Student Records* *Personnel Records* *Medical records*	*Information covered by non-disclosure agreements*	*Academic statistics*
Reputation Protection	Disclosure would cause exceptional or long term damage to the reputation of the University, or risk to those whose information is disclosed.	Could cause harm to the reputation of the University	Low risk of embarrassment or reputational harm
Examples	*Detailed Academic records* *Sensitive research projects* *Animal research details* *Disciplinary details* *Exam papers*	*Research details or results that are not strictly confidential data* *College/School evaluation* *Examination marks*	*Project related memos, information circulated to staff which is not intended as public material.* *Staff email*
Commercially sensitive	May have serious or long term negative financial impact on the University	May have short term financial impact on the university	
Examples	*Certain management information (e.g. pending organisational changes, sensitive negation positions)* *Financial records* *Papers dealing with commercially sensitive research* *Contract information with third parties*	*Management decisions* *Research Funding Information* *Detailed budgets* *Detailed financial reports* *Routine financial transactions*	*Published financial records*
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or	General university information
Examples	*Information on significant security vulnerabilities* *Detailed system technical information* *Passwords and other sensitive access credentials.*	*Information resources with access to restricted data* *Detailed operating procedures* *Draft policy or procedure documents*	*Internal Operational manuals* *Internal training Materials* *Some policy documents* *Personal directory data (e.g., contact information)* *E-mail* *Institutionally published public data* *Past exam papers*
Public/ Unrestricted	Not sensitive when released- should be subjected to internal review before issuing.		