UNIVERSITY COLLEGE CORK

Data Management Policy

Version 1

1/17/2013

This Data Management Policy is designed to help the UCC community understand their responsibilities with regards to the protection of electronic data. In particular electronic data and information belonging to, or held by, University College Cork.

Document Location

http://www.ucc.ie/en/it-policies/policies

Revision History

Date of this revision: 17/01/2013	Date of next review: 17/01/2014

Version Number/Revision Number	Revision Date	Summary of Changes
0.1	19/04/2011	Approved by Governing body
0.2	12/10/2011	Approved by OCLA
0.3	14/10/2011	Added Branding and formatting guidelines
0.4	20/11/2011	Added section on links to existing policies
0.5	22/11/2011	Added Data protection considerations
0.6	28/11/12	Edited to reflect suggested edits by John McNulty. Abstract added to cover page NH
0.7	29/11/12	Added John Morrison comments
0.8	20/12/12	Additions from IS&ER
0.9	10/1/13	Approval by IS&ERC and final clarification amendments
0.11	17/1/13	Updated with changes suggested by Academic Board

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date
Gerard Culley	Director of Information Technology	06/11/2012
John Fitzgerald	Director of Information Services	06/11/2012
John Morrison	Chair of IS & ER Committee	10/1/2013
Michael Farrell	Corporate Secretary	6/11/2012
Academic Council		1/02/2013

This policy shall be reviewed and updated on an annual basis.

1 Table of Contents

2 Purpose

The purpose of this Data Management Policy ("the Policy") is to protect the electronic data and information belonging to, or held by, University College Cork – National University of Ireland (the "University"). It aims to provide a framework within which the roles and responsibilities of those who manage or use the data and information are defined. The intention of the Policy is to enable access to data and information held by UCC, to the greatest extent possible, consistent with legislation and relevant UCC policies, whilst ensuring that electronic data is protected from unauthorised use, access and breaches of privacy. The policy is not designed to deal with the more complex matter of research data.

3 Definitions

http://www.dataprotection.ie/docs/a_guide_for_data_contollers/696.htm

3.1 Data

"Data" means information in a form which can be processed and is a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information. Please note: this Policy only refers to electronic data (i.e. data held on computer or other electronic device).

3.2 Data Controller

"Data Controller" means the organisation or body which ultimately controls the content and use of data. Under this policy, the Data Controller means the University, rather than any individual, department, school, college, administrative unit or research unit, as for legal purposes it ultimate owns and controls all Data held by the University.

3.3 Data Owner

"Data Owner" means the most senior person/individual in the department/school/college/ administrative unit/research unit within which the data is created. An exception can be made if this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area. Further explanation of this term is provided below.

3.4 Information Compliance Officer:

Provides advice on appropriate classification of personal data and on compliance with data protection obligations across the University. Acts as a liaison/advisory in conjunction with the data owner. The **Information Compliance Officer** is contactable at: foi@ucc.ie

3.5 Data Custodian

"Data Custodian" means an individual or department/school/college/administrative unit/ research unit (e.g. IT Services) to which data is entrusted on behalf of the Data Controller for the purposes of storage and/or processing.

3.6 Data User

"Data User" means any person who uses, processes, stores, manipulates data held by the University.

3.7 Processing

"Processing" means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data;
- Collecting, organising, storing, altering or adapting the data;
- Retrieving, consulting or using the data; e.g. reports generated from centrally held databases
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, deleting or destroying the data.

3.8 Data Subject

A "data subject" means an individual who is the subject of or identified in the data.

3.9 Personal Data

"Personal data" means data related to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the Data Controller. Personal data would include the age of the individual, their home address, their educational and employment history, information relating to their financial affairs, marital status. Users taking personal data outside of the University need to adhere to the Encryption guidelines, as set out in the Guidelines to encryption standards.

3.10 Sensitive Personal Data

"Sensitive personal data" means personal data relating to:

- The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.
- Whether the data subject is a member of a trade-union;
- The physical or mental health or condition or sexual life of the data subject;
- The commission or alleged commission of any offence by the data subject; or
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

A more comprehensive definition of sensitive personal data is available at https://www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm

4 Scope

This Policy governs any electronic Data held by the University, for policy information on non-electronic data please refer to UCC Records Management Policy (available at: http://ocla.ucc.ie/records/records.htm). The policy does not attempt to govern research data and a subsequent policy specific to research data will be created for this purpose.

The Policy has been formulated on the basis of the following principles:

Data generated and/or held by the University are key strategic assets that must be correctly managed and controlled so as to ensure their availability, integrity and confidentiality and to protect the University's resources, reputation, legal position and ability to conduct its business.

In addition to its legislative responsibilities, the University values the privacy of the individual and the management of Data must be handled in way that protects that privacy.

For the purposes of this policy:

- Staff means all full-time and part-time employees of the University, including staff funded externally but under contract to the University.
- Students mean all full-time and part-time registered students of the University.
- External Parties means all the University's subsidiary companies, contractors, researchers, visitors and/or any other parties who are granted access to the University's IT Resources.
  (Here after collectively referred to as "**Users**")

5 Supporting Policies, Standards & Procedures

The Policy should be read in conjunction with the following University policies:

- UCC Records Management Policy (available at: http://ocla.ucc.ie/records/records.htm)
- UCC Data Protection Policy (available at: http://ocla.ucc.ie/records/data_privacy.htm)
- Policy on Externally Hosted Personal Data
- Data Classification Procedure
- IT Security Policy
- Guidelines on Encryption
- Freedom of Information procedure
- Code of Research Good Conduct

6 Data Management Policy

6.1 The Data Controller

It is the data controller's responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability.

6.2 The Data Owner

Every set of data must have a Data Owner see page 4 Data Owner. The Data Owner has overall responsibility for the quality and integrity of the data. Specifically, the Data Owner is responsible for:

- Deciding the criticality and sensitivity of the data and classifying the data accordingly (see the Data Classification Procedure see section 4 above);
- Authorising access to Data
- Authorising the use of the data, e.g. what processing takes place on the data
- Regularly reviewing access privileges
- Assessing the risks to the data
    - Risks could include but are not limited to:
        - Theft
        - Data Loss – due to lack of proper backups

        - Neglect – Old hardware being recycled without proper data sanitization
        - Online File Share
    - Data Users and Data Custodians need to be made aware of the potential consequences of data theft or loss so the relevant parties can act so as to mitigate these risks;
- Ensure that appropriate contingency plans are in place to safeguard the data and ensure that they or the Data Custodian have the appropriate backup and disaster recovery plans in place.

The Data Owner is the most senior person in the area within which the data is created unless this role has been explicitly delegated to someone else. In the case of the data for the central systems in the University, relating examples are given in this table.

Functional Area	Student Data	Staff Data	Financial data	Data warehouse	Research Data
Data Owner	Registrar	HR Director	Bursar	IT Director	Principal Investigator

Data owners must ensure that the University's Data Protection Policy (link set out in section 4 above) is adhered to at all times.

An inventory will be maintained of all the University's major electronic information assets and the ownership of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity and criticality. Sensitivity has three categories:

1. Public data, (including data under the jurisdiction of Freedom of Information)
2. Data for Internal Use Only
3. Confidential data (including Personal Data and Sensitive Personal Data)

6.3 The Data Custodian

In many cases data will be entrusted to an individual or a department/school/ college/administrative unit/research unit (e.g. IT Services) for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian. This relationship between owner and custodian is often managed by a contract or service level agreement which clarifies specific responsibilities for each party, typical Data Custodian responsibilities include:

- Maintaining the integrity and confidentiality of the data entrusted to them;
- Ensuring that access to the data is restricted to those individuals authorised by the data owner;
- Ensuring that processes undertaken on the data have been authorised by the data owner;
- Having adequate backup and recovery procedures in place for the data, taking into account the sensitivity and criticality of the data as characterised by the Data Owner ;
- Providing any information necessary for the Data Owner to fulfil their responsibilities.

6.4 The Data Users

Anyone using or processing University Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of the University (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright. The data should only be used for the purposes approved by the data owner, see Data Owner page 4.

- Data Users are responsible for protecting their access privileges – Usernames and Passwords for University Systems should not be shared
- Data generated from central systems that cannot readily be accessed externally, e.g. DMIS, ITS, and HRIS etc. should not be removed from campus without first seeking permission from the Data Owner. Data from these systems is both personal and sensitive so care should be taken when looking to access the information externally.
- Users should be especially vigilant in complying with this policy when transferring data to mobile equipment such as laptops, tablet devices, phones, USB memory sticks, PDAs, DVDs etc., as they have a greater risk of being lost or stolen.
- Anyone accessing information systems remotely to support the business activities of the University must be authorised to do so by the Data Owner of this data. (Permission can be implied given the fact that the system allows the Data User to log in remotely) The strategic importance and sensitivity of the data being accessed needs to be considered and common sense should be used in these situations.
- Removal off-site of Confidential Data must be properly authorised by the Data Owner. The potential fallout from the theft or loss of said Confidential Data should be considered by both the Data User and Data Owner before removing the data off-site. If necessary the Data Custodian (e.g. IT Services) can be consulted to ensure all possible safe guards are being used e.g. laptop encryption.
- Confidential Data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer. Please refer to UCC's IT Security Policy (link set out in section 4 above) and Guidelines on Encryption link set out in section 4 above), this procedure outlines the encryption standards recommended by IT Services.
- Unsolicited electronic mail (aka SPAM) should not be acted upon or forwarded, a definition for bulk email can be found in the bulk email procedures. If a Data User fears they may have responded to a SPAM email they should contact the staffithelpdesk@ucc.ie immediately to have their access credentials updated.
- Email addresses should be checked carefully prior to dispatch to avoid sending information to unintended users.
- Where the information contains data of a personal nature, extra vigilance is required. While it is acknowledged some users will need to process (including transmit) personal data as part of their job, all Data Users are required to comply with UCC's Data Protection Policy (link set out at section 4 above) when processing personal data. A list of Data Protection guidelines are available online at http://www.ucc.ie/en/it-policies/guidelines/

6.5 Storage Media

Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved. IT Services will advise Data Owners and Data Users as to the appropriate media type.

6.5.1 Disposing of equipment/storage media

When permanently disposing of equipment containing storage media, all Confidential Data and licensed software must be irretrievably deleted before the equipment is moved off-site.

Any third party used for external disposal of the University's obsolete data-bearing equipment must be able to demonstrate compliance with the University's information security policies. Where appropriate and/or where the data being disposed of contains Confidential Data, as categorised by the Data Owner, the third party will enter into a service level agreement which documents the performance expected and the redress available in case of non-compliance and, where it contains personal data, the data protection contractual commitments required to be given to the University by law.

7 Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk staffithelpdesk@ucc.ie. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

8 Revisions to Policy

The University reserves the right at any time to revise the terms of this Data Management Policy. Any such revisions will be noted in the revision history of the policy, which are available to you on the website and by continuing to use the University's IT Resources following any updated you will be deemed to have accepted the revised terms of this Policy.

9 Further Information

If you have any queries in relation to this policy, please contact:

Director of IT Services

University College Cork

Tel: 021 4902215

Email: it_director@ucc.ie