University College Cork

Externally Hosted Personal Data Policy

**Version 1**

**2/14/2014**

The purpose of this policy is to inform the UCC community on how to ensure the safekeeping of UCC personal data when it is hosted externally. It also outlines UCCs obligations under the Data Protection Acts and establishes a process to ensure that the University is compliant with the data protection law and that associate data risks are managed appropriately.

**Document Location**

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

**Revision History**

|  |  |
| --- | --- |
| **Date of this revision: 16/10/2013** | **Date of next review: 16/10/2014** |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Version Number/Revision Number** | **Revision Date** | **Summary of Changes** |
| 0.1 | 31/10/2012 | Redraft using standard template |
| 0.2 | 26/11/2012 | Redraft based on feedback from OCLA |
| 0.3 | 03/12/2012 | Amend after ICT DP Meeting & corrections from COS |
| 0.4 | 22/3/2013 | Amendments from IS&ER committee |
| 0.5 | 30/4/2013 | Further Amendments to the policy from IS&ER feedback |
| 0.6 | 21/5/2013 | Amendments from OCLA and IS&ER committee |
| 0.7 | 28/05/2013 | Final amendment’s from OCLA |
| 0.8 | 09/08/2013 | Changes requested by Academic Board |
| 0.9 | 17/09/2013 | Changes requested by College of business and law |
| 0.11 | 16/10/2013 | Including changes referencing University Ethics Committee |
| 1.0 | 14/02/2014 | Approved |

**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 |  |
| John Fitzgerald | Director of Information Services |  |
| John Morrison | Chair of IS & ER Committee  |  |
| Michael Farrell | Corporate Secretary |  |
| Heads of College |  |  |
| Academic Council |  |  |

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

Table of Contents

[1 Purpose 5](#_Toc380131432)

[2 Definitions 5](#_Toc380131433)

[2.1 Data 5](#_Toc380131434)

[2.2 Processing 6](#_Toc380131435)

[2.3 Personal Data 6](#_Toc380131436)

[2.4 Sensitive Personal Data 6](#_Toc380131437)

[2.5 UCC Personal Data 6](#_Toc380131438)

[2.6 Data Controller 6](#_Toc380131439)

[2.7 Data Owner 7](#_Toc380131440)

[2.8 Data Custodian 7](#_Toc380131441)

[2.9 Data User 7](#_Toc380131442)

[2.10 Data Subject 7](#_Toc380131443)

[3 Scope 7](#_Toc380131444)

[4 Supporting Policies, Standards and Procedures 7](#_Toc380131445)

[5 Externally Hosted Personal Data Policy 9](#_Toc380131446)

[6 Roles and Responsibilities 10](#_Toc380131447)

[6.1 Users 10](#_Toc380131448)

[6.2 Office of Corporate and Legal Affairs 10](#_Toc380131449)

[6.3 Information Compliance Officer: 10](#_Toc380131450)

[6.4 IT services 10](#_Toc380131451)

[7 Breach of This Policy 11](#_Toc380131452)

[8 Revisions to Policy 12](#_Toc380131453)

[9 Further Information 12](#_Toc380131454)

# Purpose

Software as a Service (SaaS), cloud and hosted services often require the storage of personal data, which is under the control of UCC. However, UCC‘s obligations to safeguard this data, under the Data Protection Acts, 1988 and 2003 (‘the Data Protection Acts’) remain unchanged. Therefore the risk of data loss or inadvertent exposure of personal information must be assessed and managed as part of any deployment of these service models.

The purpose of this policy is to ensure the safekeeping of personal data which is controlled by UCC, when it is hosted externally and that UCC fulfils all its obligations under the Data Protection Acts.

The document specifically applies to the third party hosting of large datasets which contain personal data. To achieve this, where appropriate UCC must ensure that for each external hosting arrangement a contract is in place that ensures.

1. the appropriate controls are in place to approve and manage the transfer of UCC personal data,
2. the data security needs and risks are assessed in each instance,
3. the external service provider has the requisite IT security measures in place, and

If an appropriate internal UCC IT solution can be provided, this is the preferred solution, particularly where there are data protection considerations. Where an external solution is deployed, the policy outlines a set of reasonable controls to help safeguard the data. This policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

# Definitions

The following definitions are defined by the Irish Data commissioner website, please note link below. <http://www.dataprotection.ie/docs/a_guide_for_data_contollers/696.htm>

These definitions are based on the Irish Data Protection act and Data Protection amendment Act, (see section 4 for more details).

## Data

“Data” forms part of the definition of personal data below. It means information in a form which can be processed (defined below) and includes both automated data (which means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer) and manual data (which means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system). Please note: this Policy only refers to electronic personal data (i.e. personal data held on computer or other electronic device).

## 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;
* Disclosing the information or data by transmitting, disseminating or otherwise making it available;
* Aligning, combining, blocking or erasing the data.

## 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, etc.

## Sensitive Personal Data

“Sensitive personal data” is afforded a higher level of protection under the Data Protection Acts. It means personal data relating to:

* Racial or ethnic origin, political opinions or the religious or philosophical beliefs of the data subject;
* 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.
* 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
* Whether the data subject is a member of a trade-union;

## UCC Personal Data

UCC Personal Data means personal data collected and controlled by UCC as part of its teaching, research, administrative and/or related functions.

## Data Controller

“Data Controller” means the body which ultimately controls the content and use of personal data. Under this policy, the Data Controller means UCC (rather than any individual, department, school, college, administrative unit or research unit), as for legal purposes UCC ultimately controls all UCC personal Data (and requires all Data Users to adhere to the Data Protection Acts).

## Data Owner

“Data Owner” means the most senior person in the department/ school/ college/ administrative unit or research unit within which the data is created or stored unless 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 classification, quality and integrity of the data held in their area. Further explanation of this term is provided below.

## 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.

## Data User

“Data User”, hereafter referred to as “User” means any person who processes data held by the University.

## Data Subject

A “data subject” means an individual who is the subject of personal data.

# Scope

This policy is limited to electronic personal data, covering both personal and sensitive personal data as defined above and in the Data Protection Acts. It applies whenever external services are used to host UCC personal data i.e. on IT infrastructure not directly managed and controlled by UCC. It applies to all staff and third parties with access to UCC personal data.

For the purposes of this Policy:

* Staff means all full-time and part-time employees 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 and/or University social media sites/discussion forums on third party platforms.

(Hereafter collectively referred to as “**Users**”)

# Supporting Policies, Standards and Procedures

The Policy should be read in conjunction with the following University policies and Users should ensure compliance with these policies in addition to this policy:

* Data Protection Act, 1988 - <http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html>
* Data Protection (Amendment) Act 2003- <http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html>
* [UCC Records Management Policy](http://ocla.ucc.ie/records/rm_policy_doc.html) -http://ocla.ucc.ie/records/rm\_policy\_summary.html
* [UCC Data Protection Policy](http://ocla.ucc.ie/records/data_privacy.htm) – <http://www.ucc.ie/en/policiesandprocedures/itsystems/>
* UCC Acceptable Use Policy – <http://www.ucc.ie/en/media/support/itpolicies/policies/AcceptableUsagePolicy.pdf>
* UCC Data Management Policy – <http://www.ucc.ie/en/policiesandprocedures/itsystems/>

# Externally Hosted Personal Data Policy

All Staff have a duty to safeguard UCC personal data in conformance with UCC’s Data Management Policy and must consult, in the first instance, with IT Services before transferring any personal data for external processing, storage or transmission. Appendix 1 offers a detailed workflow of steps required by staff when requesting to externally host personal data. Before hosting data externally users must recognise the risks of using cloud services to store personal data and as a matter of due diligence, perform the checks and steps outlined below:

1. Requests for external hosting of UCC personal data must be submitted to IT Services for approval, requests should be emailed to helpdesk@ucc.ie where they will be forwarded to the appropriate contact point within IT Services.
2. Users must ensure that personal data is capable of being, and will be encrypted during transfer to the hosting party.
3. The UCC Data Owner must approve the transfer of personal data and the frequency thereof. Where there is no defined Data Owner, personal data cannot be stored on external systems.
4. Sensitive personal data can only be hosted externally if the service provider is certified to an approved IT Security standard (typically ISO 27001).
5. In relation to personal data that does not fall into the category of sensitive personal data, the external service provider should ideally be certified to recognised international IT Security standards (typically ISO 27001), as per point 4. In the absence of certification, a risk assessment must be carried out. This can be assessed with a security questionnaire or, in exceptional cases, by undertaking an independent security audit. Any costs associated with an independent audit will need covered by the user. The final decision on the acceptability of the service provider’s security arrangements will rest with the Third Party Hosting Group (see below).
6. Data must be stored within the EU; unless the Office of Corporate and Legal Affairs (OCLA) are otherwise satisfied e.g. the country where the data will be stored has been deemed by the EU to have an adequate level of data protection.)
7. A list of approved service providers will be developed and maintained by IT Services and published for the benefit of users on a dedicated University webpage. Users of an approved provider can simply notify the compliance officer (foi@ucc.ie), so that they can update the register of the location of all personal data.
8. In the event of any dispute, the UCC Data Classification procedure OCLA will determine if any item of data is deemed to be personal.
9. A data processing agreement that is acceptable to, and signed-off on, by the Office of Corporate & Legal Affairs must be in place the external service provider prior to any transfer of personal data to a service provider for the purpose of hosting or otherwise processing personal data on behalf of UCC.

# Roles and Responsibilities

## Users

1. Ensure that UCC personal data is not provided to external service providers or stored externally without obtaining the prior approval of the data owner,
2. Liaise with IT Services before availing of any externally hosted service requiring the transfer of UCC personal data, and
3. Provide the business case, the details of the service provider, the personal data fields to be transferred, and the frequency of transfer to the chair of Third Party Hosting Group.

## Office of Corporate and Legal Affairs

1. Arbitrates and ultimately decide on the classification of data, (Personal, Sensitive, Public), where a consensus cannot be reached.
2. Validates the bona fides of the external service provider, in conjunction with IT Services.
3. authorises the personal data fields to be externally hosted,
4. act as the authorised signatory and approval authority for Data Processing Agreements with service provider who it is proposed will host or otherwise process UCC personal data on behalf of UCC,
5. give final approval for the transfer, and
6. Maintain the register of externally hosted personal data.

## Information Compliance Officer:

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

## IT services

1. Determine if the external service provider has the appropriate IT Security certification,
2. Determine where the data is to be located,
3. Liaise with the Data Owner and OCLA to carry out an appropriate risk assessment,
4. Ensure that the requisite IT Security measures are in place to safeguard data in transfer and storage, and
5. Determine the frequency of IT audits, if required.

The responsibilities of OCLA and IT Services with regard to carrying out a risk assessment where a proposed service provider does not possess a recognised/acceptable IT security standard will be discharged jointly through the formation of a Third Party Hosting Group. This group will also contain representatives of UCC System Administration. The members of this group are:

* Director of IT Services (Chair)
* Officer, OCLA
* Head of Enterprise Applications, IT Services
* Head of Academic Systems Administration, Registrar’s Office
* Systems Administrator representative

This group retains full discretion on engagement with any service provider based on the output of the risk assessment. The quorum for meetings of this group shall be four and any decision by this group must be approved by the majority of the members in attendance.

 Note that where ethical questions pertaining to the data are raised by an application to this group, the matter will be referred to the University Ethics Committee for consideration.

# Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this policy immediately to IT Services Helpdesk (email: HelpDesk@cc.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 the University’s Data. In addition to the above, if any breach of this policy is observed, disciplinary action up to and including dismissal (in the case of staff), or contract termination (in the case of third parties) may be taken in accordance with the University’s disciplinary procedures for staff as appropriate.

# Revisions to Policy

The University reserves the right at any time to revise the terms of this Externally Hosted Personal Data 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.

# 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