Data Protection
Key Points for DCU Researchers

Introduction

Purpose & Intended Audience
This guide is intended to provide guidance to DCU's Research Community on the key data protection points to consider when conducting research that involves personal data. It should not be construed as legal advice but any queries you may have should be taken up with the University's Data Protection Unit.

The term 'Research Community' should be read in the broadest sense and it is intended to refer to all researchers engaged in research at DCU, whether as pure research, or in connection with a course of study at either undergraduate or postgraduate level.

It is acknowledged that both pure research and post graduate research are more likely to be of higher risk from a data protection perspective than research conducted as part of an undergraduate programme. Nevertheless, the key points of this guide will still apply.

What is 'Personal Data'?
Personal data is any information about a living person, where that person is either identified or could be identified, from the data itself or when it is combined with other data. Typical examples of personal data in a research context are:
a) Paper based records: e.g. consent forms, research participant files, patient records, interview notes etc.
b) Electronic records: e.g. database of participant details, online survey returns, photos, audio & visual recordings, IP addresses, diagnostic / clinical images etc.
c) Other: e.g. genetic data, biometric data, clinical or medical samples etc.

Note: Any data that is fully and completely anonymous is not considered to be 'personal data'. However, any data that is merely pseudo-anonymised (e.g. where a researcher can still link any information to an identifiable individual) is still deemed to be 'personal data'.

Legal Obligations
If personal data is to be obtained and/or processed in the course of the proposed research then there are certain legal obligations and data protection principles to be followed. These are set out in the EU's 2016 General Data Protection Regulation (GDPR) and related Irish legislation.

Key Points for Researchers

1. **Training**
   All research team members, including the Principal Investigator (PI), must complete the DCU Data Protection Training module on Loop, or an equivalent data protection training programme.

   DCU Staff and Researchers may access the online training via HR's Essential eLearning web page.

   Note: You may need to firstly enrol and then unlock the Data Protection course to access it via the University's Loop platform.

   DCU Students should navigate directly to their Loop account and select the student specific version of the course '2021/2022 Data Protection – Students'. This can be found via the search function in Loop.

Data Protection
Key Points for DCU Researchers

2. Data Protection Principles

There are a number of data protection principles to be followed whenever personal data is obtained or processed, including the processing of it for research purposes. Guidance on the principles is provided in the online training resources referred to above.

From a research perspective three of the more important principles are:

a) Data Minimisation / Limitation
Only request the minimum amount, and categories, of personal data needed to perform the proposed research and no more. Each category of personal data used needs to be justified from a research perspective. If you cannot justify it, then do not request, gather or process it.

b) Transparency
Most research involving personal data is conducted upon the consent of the participants involved. In order for consent to be valid the participants must be informed of how their personal data will be used and managed. This is usually achieved by providing a Plain Language Statement (PLS) incorporating a section on Data Privacy that is clear, accurate and at an appropriate level for the reader, especially where children are the intended participants.

c) Safe & Secure
The primary onus to keep personal data safe and secure, while it is in their possession, lies with the researcher and/or the research team. The degree and type of security applied to the data will depend upon the context, with 'sensitive' or 'special' data requiring a more robust level of security.

3. Research Ethics Approval

In line with the University's requirements for all research involving human subjects, such proposals must receive approval to proceed in advance from the appropriate DCU ethics review body (e.g. University Research Ethics Committee (REC), Faculty REC (F-REC) or a school ethics review panel). From a data privacy perspective your attention is brought to the following.

a) **Personal Data Section of the relevant Research Proposal Application Form**
Researchers must complete the Personal Data section of the relevant application form where their study involves processing personal data in any manner. For example, Section 4 of the University REC form deals with 'Personal Data'. Due care and attention must be taken when completing section 4 as it will flag any potential data protection issues early in the approval process and further scrutiny of the proposal by the DPU may be required depending upon the answers provided (see point 12 below).

Note: Faculty level RECs and School ethics review panels may have slightly different application forms to the University level REC referred to above but they should contain a section on 'Personal Data' nevertheless.

b) Plain Language Statement
From a data protection perspective, and in most cases but not necessarily all, researchers will require consent from the research participants to process their personal data. This is usually achieved by means of a signed 'Consent Form' after providing a tailored Plain Language Statement (PLS) to the participant and by answering any questions they may have prior to the participant signing the Consent Form.

Within the PLS template provided on the University's REC web page there is a sub-section titled 'Privacy Notice'. This section must be retained in the final version of the PLS used in the research and it must be

tailored to the unique circumstances of the research project. Deletion of this subsection is not an option where the research proposal involves the processing of participants personal data, either by the research team, or by any external agent used by the team to process personal data obtained during the research.

The PLS specific to the research project must be suitable for its intended audience. If the audience includes children then the PLS must be child specific and its content should be capable of being easily understood by the intended reader.

4. Consent Forms

As stated above consent will, in the majority of cases, be the legal basis invoked for the processing of the personal data of participants involved in the research. Evidence of a participant's consent to be involved in the research, and to have their personal data used in the research, will usually be achieved by having a signed 'Consent Form' on file, signed either in paper format or by electronic means. A template is provided on the University's REC web page.

As is normal with research involving individuals the participants must have the capacity to understand what they are consenting to and, in the case of a child less than 18 years old, the Consent Form must be signed by a Parent or Guardian (see point 5 below).

5. Assent Forms

Where the research participants are children, and therefore do not have the legal capacity to give their consent to the processing of their personal data, then a formal 'Assent Notice' must be provided to the child and it must be authorised or signed by the child. This is in addition to the Parent or Guardian's Consent Form referred to above in point 4. An example is provided on the University's REC web page

6. Board of Management Approval

Where the research project is to be conducted in a primary or secondary school then it is usually the case that formal approval to conduct the research is required in writing from the school's Board of Management. Ideally, such approval should also be formally noted in the minutes of the relevant meeting of the Board of Management of the School where the request to conduct research is to be discussed.

7. DCU IT Systems & External Processing

The University's computer resources should, in the majority of cases, be the host system for the research project's electronic records. If the research requires the utilisation of any external software (e.g. Zoom, Qualtrics etc.) then the research team should use the version provided through, or by, the University.

8. IT Devices & Encryption

Ideally, and wherever possible, access to all IT devices (e.g. Laptops, PCs, Voice Recorders etc.) being utilised on the research project should be controlled (e.g. by use of a password or passphrase) and wherever possible the data on the device should also be encrypted.

Where the research involves the collecting or processing of 'Special' or 'Sensitive' categories of Personal Data (e.g. data relating to an individual's sexual orientation, mental or physical health etc.) then additional and more robust security measures to protect the data may need to be put in place.

If one of the Research Team's IT devices that holds personal data is lost, stolen, destroyed or damaged, or the data is disclosed to an unauthorised person, then the DCU Data Protection Unit is to be informed immediately.

Data Protection
Key Points for DCU Researchers

9. Research Files (in Electronic or Paper format)

Where research files (e.g. participant's Consent Forms, Patient files etc.) are used in the course of the research, and they contain personal data, then secure access to the files must be managed by the Research Team. The files are to be stored in a safe and secure manner and should only be accessed by members of the Research Team. Where necessary, non-research team individuals may be allowed access but only after authorisation by the Principal Investigator.

If any research file containing personal data is accidentally lost, stolen, destroyed or damaged, or the data is disclosed to an unauthorised person, then the Data Protection Unit is to be informed immediately.

10. Third Party Processing

Where a third party external to DCU is to process personal data on behalf of the researcher or the research team then a formal Data Processing or Sharing Agreement (DPA/DSA) may need be put in place between the parties. Researchers should contact the Data Protection Unit for specific guidance to establish whether a DPA/DSA is required and the form it will take.

11. Prohibition on transferring personal data outside of the EU or EEA

As a general rule, no personal data should be shared, processed or otherwise transferred to or with any entity or organisation outside of the European Union (EU) or European Economic Area (EEA) in the course of the research study, or thereafter.

There are exceptions to this rule (e.g. data may be shared with some organisations based in the United States in limited circumstances) but as this area is complex advice from the Data Protection Unit should be obtained in advance.

12. Insider Research

Insider research is the term used to describe research in which the researcher has a direct involvement, or connection, with the research setting. The attention of researchers is drawn to the REC's Guidance on this topic.

13. Data Protection Impact Assessments (DPIA) / Health Research DPIA

In some very rare cases it may be necessary to prepare a DPIA to assess the risks to individuals from the proposed research before the research proposal can be given the approval of the DPU to proceed. This is a legal requirement and must be done where the circumstances of the research mandate it.

Where the DPU believes that a DPIA may be required, the first step will be for the researcher to complete a short DPIA Screening Questionnaire (SQ). The SQ contains a number of questions around the nature of the personal data to be processed and the intended processing. The DPU will assess the answers provided and decide whether a formal DPIA is needed.

DPIAs can take one of two forms. One is specifically for 'Health Research' and the other is for non-health related research (more common). The completion of a DPIA can take some time and involve the participation of many parties so it should only be completed where the DPU has expressly recommended doing so or where an external party involved in the research requires one (e.g. a hospital or medical clinic).

Data Protection
Key Points for DCU Researchers

Version Control

Document Name	Data Protection – Key Points for Researchers	
Unit Owner	Data Protection Unit	
Author	Risk & Compliance Officer	
Version Reference	**Original Version 1.0**	**Reviewed Version**
Approved by	Data Protection Officer	N/a
Effective Date	September 14th 2022	N/a

End.