Implementing Data Protection Principles in Research Guidelines

Section 1 - Introduction

(1) Article 5 of the General Data Protection Regulation 2016 (GDPR) sets out the key principles underpinning data protection. Compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR.

(2) The following seven principles underpinning data protection are dealt with in the Personal Data and Records Policy:

a. Lawfulness, Fairness and Transparency
b. Purpose Limitation
c. Data Minimisation
d. Accuracy
e. Storage Limitation
f. Integrity and Confidentiality
g. Accountability

Key Data Protection Terms in Research Context

(3) The following key data protection terms apply to this document:

a. Data Controller
b. Data Processor
c. Data Subject
d. Personal Data
e. Special Category Data
f. Criminal Offence Data
g. Identifiable Natural Person

Specific Considerations for Research

(4) Collecting personal data can be a large part of research collection. Consequently, it is important that safeguards are in place when conducting research in order to protect an individual's personal data. Responsibility for implementation of data protection principles extends to students and supervisors in the course of placements and research.

(5) In the unlikely event that special category data is required to be collected, e.g. information related to an individual's health, membership of a trade union, religion, political opinions and so on, additional protection is required to ensure data is not misused or disclosed to unauthorised parties.

(6) Hibernia College student or Staff research projects are not authorised to process criminal offence data.

Exemptions to GDPR Principles for Research Purposes

(7) Subject to the existence of appropriate safeguards, Article 89 of the GDPR sets out certain exemptions to the principles of data processing for research purposes. These exemptions are set out below, and the College may apply these exemptions with regard to personal data collected for research purposes, where necessary:

a. Storage Limitation: Research data can be held for an indefinite period of time.
b. Purpose Limitation: Research data can be used for a purpose other than that it was originally intended for, provided that purpose is still research.
c. Data Subject Rights: Certain exemptions as set out in Article 89 of the GDPR may apply with regard to data subject rights (see below).

(8) However, these exemptions are only applicable under the following circumstances:

a. Where complying with the above provisions would prevent or seriously impair the purpose of processing.
b. Data minimisation measures are implemented.
c. Processing is not likely to cause substantial distress or damage to an individual.
d. Processing is not used for specific measures or decisions about an individual.
e. Research results are not available in a way which identifies individuals.

(9) In the context of the College's research, these exemptions normally only apply to Staff and Faculty research. Students are not permitted to hold their data indefinitely or use research data for any other purpose other than it was originally intended.

Section 2 - Important Points to Remember When Conducting Research

Be Aware

(10) Be aware of any personal data that you collect directly or indirectly during your studies and particularly during research, and ensure that all personal data is treated confidentiality and securely.

(11) Ensure that you familiarise yourself with the Personal Data and Records Policy and that you apply the data protection principles throughout your research.

Be Prepared

(12) Prior to collecting and analysing personal data, plan appropriate measures for data collection/disclosures in line with data protection principles and the Personal Data and Records Policy.

(13) Plan the resources you will require in advance and ensure you avail of College approved and/or College licensed IT resources where they are available.

(14) Permission must be sought to use any IT resources that have not been made available by the College.

Data Breaches

(15) If you suspect that a data breach has occurred, refer to the Personal Data Security Breach Management Procedure and contact the Records and Data Manager without delay.

(16) Avoid data breaches by following good data protection practices such as using bcc only if a group email is

necessary and having a high-quality disposal routine, e.g. shredding sensitive files and disposing them in confidential waste where possible.

Data Pseudonymisation

(17) Pseudonymisation should be used where appropriate and a protected file containing the key identifying participations should be the only location where participants are identifiable in a dataset.

(18) Please find further guidance from the Data Protection Commission on anonymization and pseudonymisation here: https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation.

Section 3 - Considerations for Virtual Face-to-Face Research

(19) A number of researchers have outlined the ethical implications of conducting research and collecting data in a virtual environment, including the use of videoconferencing for online interviews and focus groups, with a particular focus on the issues of consent and anonymity of participants. Rodham and Gavin (2006) concluded that ethical issues raised when planning and implementing online data collection are no different to those raised by more traditional approaches to data collection.

(20) The following points should be considered when preparing to conduct research online:

a. Usual research guidelines and academic good practice apply in relation to consent and research participation. This includes, but is not limited to, the guidance and regulations as set out in the Academic Good Practice Policy, the Research Handbook and BERA Guidelines for Ethical Guidelines for Educational Research.
b. Informed consent – ensure all participants provide explicit consent to taking part in the research and give their permission for the researcher to record, analyse and report any data collected. The researcher must make it explicit within their ethical application how informed consent will be obtained and recorded.
c. The use of online or other technological means can be problematic as individuals can potentially conceal their identity; however, this is not necessarily any different to the use of other methods of data collection such as surveys which are reliant on participants to provide honest answers. No matter what mechanism is used to facilitate data collection in research, the integrity of the researcher and participants is paramount.
d. Participants can have a misplaced expectation of privacy when using publicly available communication systems which are, by nature, mechanisms for the storage, transmission, and retrieval of comments. Consequently, when conducting research using any online medium, it is important that privacy is addressed explicitly in terms of storage, transmission and data access.

Status and Details

Status	Current
Effective Date	2nd November 2020
Review Date	2nd November 2023
Approval Authority	Academic Board
Approval Date	23rd September 2020
Expiry Date	Not Applicable
Enquiries Contact	Ruth Ní Bheoláin Quality Assurance Officer +353 1 661 0168 Quality Assurance

Glossary Terms and Definitions

"Data Controller" - A data controller is a person or body who determines the purposes and means of the processing of personal data. In this regard, the College is the Data Controller. However, this responsibility extends to all persons using and processing personal data in relation to their work or studies with the College, where those persons determine the purposes and means of the processing of personal data.

"Data Processor" - A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Data Subject" - A data subject is an identifiable natural person who can be identified, directly or indirectly, from a dataset. As a data controller, the College and members of the College community are responsible for ensuring any processing of that personal data occurs in line with the principles at set out in this policy.

"Personal Data" - Personal data is information relating to an identifiable natural person who can be identified directly or indirectly from factors, such as name, contact details or any attributes distinguishing a person.

"Special Category Data" - Special Category Data is information relating to an identifiable natural person which requires a higher level of protection than personal data and includes personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

"Criminal Offence Data" - Criminal Offence Data is a type of data in its own right that can only be processed by an organisation that has legal authority to do so. This is information about criminal allegations, proceedings or convictions as outlined under Article 10 of the GDPR.

"Identifiable Natural Person" - An identifiable natural person is one who can be identified, directly or indirectly, from a source of data.