Hibernia College Quality Framework

Guideline for Implementing Data Protection Principles in Research

1 Introduction

Article 5 of the General Data Protection Regulation (GDPR) sets out eight 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.

The following seven principles are outlined in the Policy for Personal Data and Records but are summarised as follows:

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

1.1 Key Data Protection Terms in Research Context

a. *Definitions for the following key data protection terms can be found in the Policy for Personal Data and Records, and apply to this policy document also:*

i. Data Controller
ii. Data Processor
iii. Data Subject
iv. Personal Data
v. Special Category Data
vi. Criminal Offence Data
vii. Identifiable Natural Person

b. *Specific considerations for Research*

i. 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.
ii. 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 etc., additional protection is required to ensure data is not misused or disclosed to unauthorised parties.
iii. Hibernia College student or staff research projects are not authorised to process criminal offence data.

1.2 Exemptions to GDPR principles for Research Purposes

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:

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

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

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

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.

1.3 Important points to remember when conducting research

a. Be Aware

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

ii. Ensure that you familiarise yourself with the Policy for Personal Data and Records and that you apply the eight data protection principles throughout your research.

b. Be Prepared

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

ii. 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.

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

c. Data Breaches

i. If you suspect that a data breach has occurred, refer to the Procedure for Managing Personal Data Security Breaches and contact the Records and Data Manager without delay.

ii. Avoid data breaches by following good data protection practices such as using bcc only if a group email is necessary, having a high-quality disposal routine e.g. shredding sensitive files and disposing them in confidential waste where possible.

d. Data Pseudonymisation

i. 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.

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

1.4 Considerations for Virtual Face-to-Face Research

A number of researchers have outlined the ethical implications 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. The following points should be considered when preparing to conduct research online:

- 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 Policy for Academic Good Practice, the Research Handbook and BERA Guidelines for Ethical Guidelines for Educational Research.
- Informed consent to 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.
- 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 researcher and participants is paramount.
- 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.

1.5 References

- Rodham, K., & Gavin, J. (2006). The ethics of using the internet to collect qualitative research data. *Research Ethics*, *2*(3), 92-97. Available at: https://ethics.grad.ucl.ac.uk/forms/Rodham_RER2_3.pdf [Accessed 26/05/2020]
- Tiidenberg, K. (2018). Ethics in digital research. *The SAGE handbook of qualitative data collection*, 466-479. Available at: https://www.researchgate.net/publication/325157593_Ethics_in_Digital_Research [Accessed 26/05/2020]
- https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-overview/gdpr-and-irish-data-protection-law/
- https://www.mie.ie/en/research/research_policy/gdpr_for_research_purposes.pdf
- https://www.dcu.ie/sites/default/files/research_support/pdfs/DCU%20Data%20Protection%20Training%20-%20Research%20Students.pdf

2 Document Control

Document Title	Guideline for Implementing Data Protection Principles in Research		
Author	QA Officer		
Version	1.0	Adoption Date	15/09/2020
Expected Review Date			
Related Policies	Policy for Personal Data and Records Policy for Acceptable Use of ICT Policy for Public Information, Promotion and the Recruitment of Students		
Related Guidelines	Procedure for Managing Personal Data Security Breaches Procedure for Managing a Data Subject Access Request (DSAR) Procedure for Change of Personal Details		
Related Procedures	Document Retention Schedule HCQF Guidelines for Data Protection and the Handling of Student Data		