Hibernia College Quality Framework

## Data Protection Impact Assessment (DPIA)

# Introduction

The form is to be completed in line with the College DPIA Procedure.

## Project Outline

|  |  |
| --- | --- |
| Name and role of Staff, Faculty or Adjunct Faculty initiating DPIA |  |
| EMT member supporting DPIA |  |
| Date submitted |  |
| Data amended (if applicable) |  |

## Where an online or digital tool is being considered

|  |  |
| --- | --- |
| Name of the tool documented in the DPIA |  |
| Link(s) to any relevant website/ background information on tool |  |
| Link(s) to tool’s privacy policy |  |

# Project Description and Ownership

*Processing**can be defined* ***as accessing, collecting, using or sharing personal data.***

## Project Description

|  |  |
| --- | --- |
| Project Description | Describe the project in detail, to the best of your knowledge |
| Purpose(s) of the processing  *Remember that GDPR imposes a purpose limitation so a clear explanation of the purpose(s) is key to this document. Any additional purpose will call for an update of the DPIA.*  *e.g. Students personal data is needed for the grading process, as the purpose is to assess each student’s performance.* |  |
| Nature and scope of the processing – *How is the data collected? What is done with it?*  *e.g. the applicant fills in the application form with their grades and uploads a copy of their transcript. The grade entered is verified by the Admissions Team on the basis of the document uploaded.* |  |
| Frequency of the processing – *Is it a daily process or a once-off project limited in time?* |  |
| Number of individuals involved or affected and group identification  *e.g. All students or specific programme and/or cohort, all staff or specific group of staff, faculty or other.* |  |
| Third parties involved  *e.g. service provider, placement site* |  |
| System(s) needed to support  *e.g. by system, consider either internal IT resource or external app.* |  |

## High Risk processes

|  |  |
| --- | --- |
| High Risk processes | *Y/N* |
| Decision-making (*in relation to the data subject) – Is the project relying, even partly, on an automated process e.g. using a tool or algorithm?* |  |
| Data Matching – *Does the process involves combining, comparing or matching multiple sets of data from different sources?* |  |
| Invisible Processing – *Has the data been obtained from another source than the data subject?* |  |
| Tracking – *Is the tool analysing the* *geolocation or behaviour of data subjects?* |  |
| ****Risk of physical harm** – *Could*** *the data (not limited but including special category data, criminal convictions and offences) jeopardise the [physical] health or safety of individual(s) in the event of a data breach?* |  |
| Vulnerable users – *Does the process involve children or vulnerable data subjects?* |  |

## Ownership

*Please list all departments of the College responsible for part or all of the process.*

*Define clearly where responsibility for decision making, concrete actions, daily use and support lies. If support is shared between two teams, e.g. IT for technical matters and Student Support for content, identify the boundaries.*

|  |  |
| --- | --- |
| Responsible Person | Description of Responsibility |
| *e.g. Admissions Team* | *To prepare the list of students starting a programme* |
| *e.g. IT* | *To set up the students’ online environment ahead of the start of the programme.* |
|  |  |
|  |  |
|  |  |
|  |  |

# Description of the data

*Please list all items of personal data processed, the rationale for doing so and the way each will be processed.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data | Rationale | | Processing action(s) | |
| *e.g. student number* | | *e.g. to allow the identification of students* | | *e.g. used as pivot data with the Student Information System.* |
|  | |  | |  |
|  | |  | |  |
|  | |  | |  |
|  | |  | |  |

# Transparency, lawfulness and fairness

## Transparency and Fairness

|  |
| --- |
| Awareness |
| Is the data subject the source of the data?  Describe how the data subjects are made aware of their data being processed e.g. data policy accessible on website, contract, ad-hoc communication.  *If a specific communication is planned, attach the text and planned means of communication, to this form.* |
|  |

|  |  |
| --- | --- |
| What are the benefits of the project? | Project Description |
| ****For the data subjects**** |  |
| ****For the College**** |  |

## Lawfulness – Personal data

For data processing to be lawful, it has to be underpinned by at least one legal basis for processing as planned by GDPR (Art. 6). Please select the relevant one(s) from the list below and explain why it applicable.

|  |  |
| --- | --- |
| Legal basis for processing | *Y/N with explanation where applicable.* |
| Consent *(if choosing this option, describe how the consent is being recorded and how the right to withdraw will be made available).* |  |
| Performance of a contract |  |
| Compliance with a legal obligation |  |
| Vital interests of the subject or another person |  |
| Public interest or exercise of public authority |  |
| Legitimate interests of the College |  |

## Lawfulness – Special Category of Data

Special Category of Data (or Sensitive Data) is data related to:

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union memberships
* Genetic, biometric or health data
* Sex life or sexual orientation

In addition to the previous table, if special category data is processed, please describe on which basis.

|  |  |
| --- | --- |
| Type of Consent | Project Description |
| Explicit consent (if choosing this option, please describe how consent is recorded) |  |
| If not planning for explicit consent, under exceptions planned by GDPR Article 9, please consult with the Data Protection Officer for further guidance. |  |

# Data minimisation

|  |  |
| --- | --- |
| Data minimisation | Project Description |
| Necessary vs Optional  Is all the personal data processed and detailed in Step 3 ‘Description of the data’ necessary?  If some of the personal data is “nice to have”, rather than necessary, please describe how data subjects are informed of the optional nature of this data set and how its voluntary processing is accommodated.  *e.g. A picture is mandatory for the establishment of the student card. It is “nice to have” on a social platform account.* |  |
| Alternative  Is there another way to achieve the same process?  *e.g. In a case where a new system or tool is proposed, consider the procedure, workload and capacity aspects of same and justify why an existing resource cannot be used.* |  |

# Data accuracy

|  |  |
| --- | --- |
| Creation and maintenance | Project Description |
| Is the personal data sourced from a controlled system (e.g. Student Information System)? |  |
| If so, how is it integrated in the project? In the case of personal data potentially changing over time, i.e. do you ensure continuous integration or reconciliation? |  |
| Does the data subject have a direct access to view and / or edit their information? |  |

# Data security, access security, organisational measures and location and sharing

|  |  |
| --- | --- |
| Data storage and Documentation | Project Description |
| How is the data stored?  *Please describe the data access management (e.g. do you need an account? Are there different levels of permissions in system? Who is managing access to the system?).* |  |
| Geographic location of the data  When using a third-party resource, it is important to consider not all jurisdictions have the same approach to data protection. Specific contractual clauses must be in place for processing out of the EU |  |
| Pseudonymisation / Anonymisation  Is there a process for either pseudonymisation or anonymisation in place?  If so, describe the method chosen. |  |
| Documentation  Describe the documentation available on the project. Include links.  *e.g. SOPs, user manuals, guidelines.* |  |
| Does the project align with existing [HCQF](https://qualityframework.hiberniacollege.com/) policies, procedures or other resources? Where a project may results in a change being needed to the HCQF, the QA Officer needs to be consulted. |  |

|  |  |
| --- | --- |
| Third party | Project Description |
| Is there a third party involved in the processing?  Third parties can be either contractors (*e.g. adjunct faculty)* or external IT resources (*e.g. an external platform, an app).* |  |
| Please define the role of the third party. Describe the control the third party and the College each have over the data. |  |
| Is there a legal agreement in place with specific data related clauses?  Does the third party have its own template?  Do you need to prepare one?  *The draft agreement must be provided for review before signature*. |  |

# Data retention and disposal

|  |
| --- |
| Data Retention and Final Disposal |
| Is the data processed already captured by the [Data Retention Schedule](https://qualityframework.hiberniacollege.com/download.php?associated=1&id=125&version=2)?  *If yes: is the planned disposal (retention period and final status) directly applicable to the project?*  *If no: propose a retention period and a disposal mechanism. If the retention period or if the final disposal differs from the existing retention schedule for similar data, please describe the rationale for the difference.* |
|  |

# Training

*Please describe the training provided in relation to the project.*

|  |  |
| --- | --- |
| Type of Training | Description |
| Internally  *e.g. IT Helpdesk trained to be able to help users, student admin support trained to use a new tool* |  |
| Externally  *e.g. Students being trained to use a new tool* |  |

# Additional information

|  |
| --- |
| Describe any additional information you believe is related to personal data, or key finding you would like to highlight.  *For instance, desk study findings demonstrating successful adoption of the same tool in reputable peer institutions. If the process or tool might be subject to public concerns, summarise why the proposed approach is answering same. If you have held a public consultation on the tool, please document.* |
|  |

# Risks identified and Outcome

Risks are individual to each project and process. Please ensure you complete a risk assessment of the process or tool to identify risk(s) to individuals or the College.

See below for an indicative list. Please note this list is **non-exhaustive.**

**Risks to individuals**

* Hacking of computers or systems
* Context of information or knowledge around process can be altered overtime, leading to data being used for another purpose than initially planned.
* New tools adopted in emergency e.g. due to Covid-19
* Combination of data sets might not allow the individual to have a fair understanding of how their personal data is used.
* Third party resources might collect users’ data wider than initially planned
* Different users might have different appetites for privacy depending on individual circumstances
* Duplication of a similar data set across systems creates a higher risk
* If a retention period is not established clearly, data might be retained and therefore used or be put at risk for longer than necessary.

**Risks to the College**

* Non-compliance with data protection or other legislation can lead to sanctions, fines and reputational damage.
* It is more difficult, hence likely more costly in terms of resources, to implement controls or changes after a process is started.
* The excessive use of personal data and feeling of “loss of control” might prevent users from engaging the College.
* Data breaches with adverse effects on individuals could lead to claims for compensation.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk identified | Risk Rating | Mitigating Measure | Risk rating  after mitigating Measure |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Should any risk be rated high and no mitigating measure can be identified, the Data Protection Commissioner needs to be consulted.

# Sign off:

|  |  |  |
| --- | --- | --- |
| Role in DPIA | Name | Signature |
| Staff, Faculty or Adjunct Faculty initiating DPIA |  |  |
| EMT member supporting DPIA |  |  |
| DPO |  |  |