STRANMILLIS UNIVERSITY COLLEGE

A College of Queen's University Belfast

DATA PROTECTION POLICY

Version No:	Reason for Update	Date of Update	Updated By
1	New Policy	June 2013	HR Manager
2	Updated Policy	June 2015	HR Manager
3	Updated Policy: In line with updated Information Security Policy and Data Protection legislation	For approval F&GP May 2021	HR Manager
4	Updated Policy	January 2025	Head of HR

Table of contents

Contents

1. Introduction

1.1. This policy provides a framework for ensuring that the Stranmillis University College meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

1.2. Stranmillis University College complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

1.3. In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

1.4. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes over-arching documents such as;

- Information Security Policy
- Retention and Disposal Policy

2. Purpose and Scope

2.1 In carrying out its responsibilities, the University College will be required to process certain information about individuals such as staff, students, graduates and other users, defined as “data subjects” in the Act.

2.2 Staff and students, or others who process or use any personal information on behalf of the University College (“data users”), have an individual responsibility to ensure that they adhere to the University College’s Data Protection Policy.

2.3 Any breach of this Policy, by a member of staff or student, can be considered as a disciplinary matter.

2.4 The GDPR defines both personal data and special category personal data (please refer Appendix 1, Definitions). The reasons for collecting and using personal data must be recorded in the Information Asset Register and must be used only of the purposes for which it has been collected and in line with the

principle of GDPR and the Data Protection Policy. Special Category Data may only be processed under specific conditions, (Refer to Section 4 and Appendix 2)

3. Principles and General Guidance

3.1 University College staff and students, or others who process or use any personal information on behalf of the University, must comply with the six Data Protection Principles. These define how data can be legally processed. "Processing" includes obtaining, recording, holding or storing information and using it in any way.

3.2 Personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which those data are processed;
- Processed in a manner that ensures appropriate security of the personal data.

3.3 All personal data held on behalf of the University, whether electronically or on paper, must be kept securely. Personal data must not be disclosed to any unauthorised third party by any means, accidentally or otherwise.

3.4 Where staff are unsure as to the whether they can legitimately share/disclose personal data with other individuals, either within or outside the University College, they must seek advice from their line manager. Further guidance is also available from the Data Protection Officer, dataprotection@stran.ac.uk.

4. Lawful basis for processing

4.1 The University College will identify the lawful basis for processing personal data and this will be recorded on Information Asset Registers.

4.2 The lawful basis for processing are set out in Article 6 of the GDPR and at least one of these conditions must apply whenever the University College processes personal data. The conditions are as follows:

- **Consent:** the individual has given clear consent to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract which you have with the individual, or because they have asked you take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the University to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary to perform a task in the public interest or official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests of the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply where the University is processing data to perform official tasks).

The University College will provide information to data subjects about the lawful basis for processing within a privacy notice.

Special Category Data

The GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Special category data may only be processed one of the specific conditions in Article 9 of the GDPR is met. These are set out in Appendix 2.

5. Rights of data subjects

5.1 Data subjects are afforded a number of rights under the GDPR. These are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automate decision making and profiling.

5.2 The right to be informed

The University College will inform data subjects, typically through a privacy notice, - show personal data held by the University College, whether obtained directly or not, is processed.

The information the University College will supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child;
- Free of charge.

5.3 The right of access

Data subjects will have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;

The University College will provide a copy of the information free of charge.

A “reasonable fee” may be required or a request may be refused where it is manifestly unfound or excessive, particularly if repetitive.

If a request is refused an explanation as to why will be provided and the data subject will be informed of their right to complain to the Information Commissioner.

If necessary, the identity of a data subject may be verified before release through the provision of relevant identification documents. Where possible and proportionate the University College will provide the data requested in the preferred format of the applicant.

Whilst data subjects have the general right of access to their own personal information which is held, the University College will be mindful of those circumstances where an exemption may apply and, in particular, the data protection rights of third parties who may also be identifiable from the data being requested.

Requests to access personal data can be made via email to dataprotection@stran.ac.uk and will be responded to within one month.

5.4 The right to rectification

The University College will rectify personal data where it is inaccurate or incomplete.

A request for rectification can be made via email to dataprotection@stran.ac.uk and will be responded to within one month.

Where a request is particularly complex the University College may request an extension, up to an additional two months.

Where the University College cannot take action to rectify an explanation will be provided to the data subject and they will be informed of their right to complain to the Information Commissioner.

5.5 The right to erasure – also known as “the right to be forgotten”

Where there is no legitimate reason for the continued processing of an individual’s personal data the University College will delete or remove the personal data at the request of the data subject.

Data may be erased to prevent processing in the following circumstances:

- When the individual withdraws consent (where consent has been provided).
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data has to be erased in order to comply with a legal obligation.
- A request for erasure may be refused where the personal data is processed for the following reasons:
- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest,
- scientific research historical research or statistical purposes;
- or • the exercise or defence of legal claims.

5.6 Right to restrict processing

The University College will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we will restrict the processing until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the College is considering whether its legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the data subject requires the data to establish, exercise or defend a legal claim.

The University College will inform the data subject if it is decided to lift a restriction on processing.

5.7 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services and allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Where the data requested meets these requirements the University College will provide the personal data in a structured, commonly used and machine-readable form and free of charge.

If the data subject requests it, the University College will transmit the data directly to another organisation, if this is technically feasible.

The University College will respond without undue delay, and within one month. This can be extended by two months where the request is complex or we have received a number of requests.

5.8 Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

The University College will stop processing the personal data unless:

- There is compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Where appropriate the University College will inform individuals of their right to object in our privacy notice.

The University College will stop processing personal data for direct marketing purposes as soon as we receive an objection.

Where the University College is conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

5.9 Rights related to automated decision-making including profiling. Where automated decision making is used and a data subject wishes to have an automated decision reconsidered, they may submit a request via email to dataprotection@stran.ac.uk

6. Security

6.1 The security of personal information in the possession of the University College is of paramount importance. In addition to the principles and procedures contained within this policy, staff and students are also advised to read and adhere to the University College's Information Security Policy.

7. Responsibilities

7.1 Information Asset Owners

Information Asset Owners have responsibility for ensuring that:

- Their staff carry out their responsibilities in this area
- All Data Protection breaches are notified to the Data Protection Officer with any remedial action taken to mitigate the risk of reoccurrence
- That mechanisms are put in place to protect data (and particularly special category data) during day to-day operations
- All personal data held within Departments is kept securely and is disposed of in a safe and secure manner when no longer needed
- All categories of personal data collected and processed are recorded on the relevant Information Asset Register
- A Data Protection Impact Assessment will be carried out for all new or updated forms of data processing and where the data processing is 'high risk'.

7.2 Data Protection Officer has responsibility for ensuring that;

- Monitoring and updating Data Protection Policy and procedures on a regular basis.
- Ensuring appropriate training is delivered to all staff on a regular basis.
- Responses to requests for information and related compliance matters are dealt with in a timely manner and in line with the requirements of data protection legislation.
- Advice on any area of the policy or data protection legislation is provided to staff and students, on request.
- Data Protection Impact Assessment are reviewed and complete.
- A log of data breaches is maintained and breaches are reported to the ICO and the Governing Body Audit and risk Committee where necessary.

7.3 The Principal/ Accounting Officer has responsibility for ensuring that;

- The University College has the appropriate policies and procedures in place to ensure compliance with the necessary legislation and;
- Informing the Governing Body on a regular basis, offering assurances in respect to compliance.

7.4 Staff Responsibilities

All staff must take personal responsibility for ensuring that:

- They are aware of their responsibilities in this area, and where they are uncertain of their responsibilities, they refer this to their line manager
- Personal data relating to any living individual which they hold or process is kept securely.
- Personal data relating to any living individual is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- All Data Protection breaches are notified to their line manager with remedial actions implemented to mitigate the risk of reoccurrence
- Personal data which they provide in connection with their employment is accurate and up-to date, and that they inform the University of any errors, corrections or changes, for example, change of address, marital status, etc.

7.5 Student Responsibilities

All students must take personal responsibility for ensuring that:

- When using University's facilities to process personal data (for example, in course work or research), they seek advice from their Supervisor/Advisor of Studies on their responsibilities in relation to Data Protection.
- Personal data which they provide in connection with their studies is accurate and up-to-date, and that they inform the University of any errors, corrections or changes, for example, change of address, marital status, etc.

8. Retention and Disposal of Personal Data/ Records

8.1 The GDPR places an obligation on the University College to exercise care in the disposal of personal data, including protecting its security and confidentiality during storage, transportation, handling, and destruction.

8.2 All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Personal data must be confidentially disposed of either via confidential waste or shredding. Consideration should be given to the nature of the personal data involved, how sensitive it is, and the format in which it is held.

8.3 The GDPR places an obligation on the University College not to hold personal data for longer than is necessary. Records should be held and disposed of in accordance with the University College retention and disposal schedule

9. Transfer of Data Outside the University College.

9.1 If personal data must be shared routinely with other organisations in order to conduct business, a data sharing agreement may be required. All new arrangements for systematically and routinely sharing data will require a data sharing agreement. Please contact the Data Protection Officer.

10. Use of CCTV

10.1 For reasons of crime prevention and security, a network of surveillance cameras including, body worn cameras, are in operation throughout campus. The presence of these cameras may not be obvious. However, signage is placed throughout campus to notify individuals that cameras are in operation.

This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out by a limited number of specified staff;
- The recordings will be accessed only by authorised personnel;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

11. Related Policies/ Documents

11.1 This policy should be read in conjunction with:

- Information Security Policy
- Information Security Breach Procedures
- Acceptable Use Policy
- University College Privacy Notices
- Retention and Disposal Policy
- Retention and Disposal Schedule

12. Review

This policy will be reviewed every three years from date of approval or in accordance with updated legislation.

Date Approved by Governing Body: January 2025

Date Review: January 2028

Appendix 1 - Definitions

Data

Information which is being used or held in a computerised system, or a 'relevant filing system' i.e., a manual filing system that is structured in such a way that data contained within it is readily accessible.

Data can be written information, photographs, fingerprints or voice recordings.

Personal Data

Information relating to natural (living) persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

Special Category Data

Personal data consisting of information as to race/ethnic origin; political opinion; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; sexual orientation; genetics and biometrics (where used for ID purposes).

Processing

Anything which can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.

Data Subject

An individual who is the subject of personal data. This will include: staff, current and prospective students, graduates, suppliers of goods and services, business associates, conference delegates, survey respondents etc.

Appendix 2: Processing Special Category Personal Data

Article 9 of GDPR lists the conditions for processing special category data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

Appendix 3: ICO List of High-Risk Processing requiring a Data Protection Impact Assessment to be carried out in line with ICO Guidance.

The ICO is required by Article 35(4) to publish a list of processing operations that require a DPIA.

1. **Innovative technology**: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI). A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
2. **Denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
3. **Large-scale profiling:** any profiling of individuals on a large scale.
4. **Biometrics:** any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
5. **Genetic data:** any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
6. **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
7. **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
8. **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
9. **Targeting of children or other vulnerable individuals:** the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
10. **Risk of physical harm:** where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.