Appropriate Use Of Special Category And Criminal Offence Data – Privacy Notice

Process Area	**Business Systems**
Reference Number	**BUS/001 Privacy Notice**
Directorate	**Finance & Planning**

Issue No	Date	Details	Author	Approved
001	May 2025	First Issue	LC, IB	SMT

1. Introduction

When processing personal data, the College will comply with the requirements of the UK General Data Protection Regulations (UKGDPR), the Data Protection Act 2018 (DPA) and any associated legislation.

In some instances, the College is required to process special category data and criminal offence data. These types of data are afforded additional protection under the DPA 2018 and UKGDPR, and the College can only process if and when certain conditions are met.

Schedule 1, Part 4 of the DPA outlines the requirement for organisations to have an appropriate document when processing special category data and criminal offence data to demonstrate that the conditions comprised within Sections 10, 11 and Schedule 1 of the DPA are met. The purpose of this Notice is to fulfil that requirement in respect of:

- Explaining the College's policies and procedures for ensuring compliance with the Article 5 Principles of the UKGDPR; and
- Explaining our policies and procedures regarding the retention and erasure of personal data.

This document complements the College's Data Protection Policy and Privacy Notices and provides detail of how the College processes special category and criminal offence data at a more granular level.

Special category data

The DPA outlines safeguards for the processing of sensitive special category data. Sensitive processing is defined in s.35(8) as:

- The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- The processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual.
- The processing of data concerning health.
- The processing of data concerning an individual's sex life or sexual orientation.

When processing special category data, the College will ensure it has identified its lawful basis for processing as set out in Article 9 of the UKGDPR including:

- for employment, social security and social protection purposes.
- for substantial public interest purposes.
- for archiving, research or statistics purposes.

Criminal offence data

Article 10 of the UKGDPR covers processing in relation to criminal convictions and offences or related security measures. The UKGDPR specifically refers to "personal data relating to criminal convictions and offences or related security measures". This covers a wide range of information about criminal activity, allegations, investigations and proceedings. In addition, Section 11(2) of the DPA specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

2. Relevant Schedule 1 Conditions and Data Processing Activities

The College relies on DPA Part 1 Schedule 1 conditions to process special categories of personal data, for example:

2.1 Conditions Relating to Employment, Health and Research, etc.

- Employment, social security and social protection:
  - Processing personal data concerning health in connection with the College's rights under employment law.
  - Processing data relating to criminal convictions in connection with the College's rights under employment law in connection with recruitment, discipline or dismissal.
  - Providing human resources and occupational health facilities for employees.
  - Substantial Public Interest Conditions.

- Statutory and government purposes:
  - Processing is necessary for reasons of substantial public interest.
  - Including processing to ensure the College's compliance with Disability Discrimination Act (1995) and other legislative requirements.

- Equal Opportunity or treatment
  - Processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment.

- Preventing or detecting unlawful acts
  - Processing necessary to ensure the safeguarding and protection of the College's students, by virtue of Paragraph 36 of Schedule 1 of the DPA it is not necessary to demonstrate a substantial public interest in the above processing.
  - Criminal offence data or personal data disclosed under for the purposes of preventing or detecting unlawful acts is shared securely and only the minimum amount of information as necessary is disclosed.

- Regulatory requirements relating to unlawful acts and dishonesty etc.
  - Assisting authorities in connection with their regulatory requirements.

- Preventing fraud
  - Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

- Safeguarding of children and individuals at risk
  - Carrying out risk assessments and processing AccessNI checks for staff and students.
  - Sharing information with relevant agencies if required.

- Insurance
  - Processing of personal data which is necessary for an insurance purpose and for reasons of substantial public interest; and
  - Where the College cannot reasonably be expected to obtain consent from the Data Subject.

- Occupational Pensions
  - Fulfilling the College's obligation to provide an occupational pension scheme.
  - Determining benefits payable to dependents of pension scheme

members.

- Disclosure to elected representatives
  - Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

2.2 Additional Conditions Relating to criminal convictions (DPA Schedule 1, Part 3).

- Extension of conditions in of DPA Schedule 1, Part 2 referring to substantial public interest.
  - The College may process personal data relating to criminal convictions in connection with its legislative obligation.

3. Procedure for ensuring compliance with UKGDPR Article 5 Principles

Article 5 of the UKGDPR sets out the data protection principles. These are our procedures for ensuring that we comply with the principles.

Principle (a) - *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*.

Processing personal data must be lawful, fair and transparent. The College provides clear and transparent information about why we process personal data including our lawful basis for processing in our Privacy Notices and in this specific document.

Our processing for the purposes of employment relates to our obligations as an employer.

Our processing for purposes of substantial public interest is necessary in order for the College to carry out its functions.

The College will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful.
- Only process personal data fairly and for the purposes disclosed to the data subject.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent.

Principle (b) - *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

Personal data must only be collected for specified, explicit and legitimate purposes and not further processed for purposes incompatible with the original purpose it was collected for.

The College will:

- only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice at the point of data collection and on the College website.
- not use personal data for outside of the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform and seek the consent of the data subject first.

Principle (c) - *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

Personal data must only be collected for the relevant purposes and must not be excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

The College will:

- Only collect the minimum personal data required for the purpose for which it is collected.
- Ensure that the personal data collected is adequate and relevant.

Principle (d) - *Personal data shall be accurate and, where necessary, kept up to date.*

Personal data must be accurate and up to date. If the College becomes aware that personal data is inaccurate or out of date, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

The College will:

- Ensure the accuracy of personal data and kept up to date where necessary.
- Ensure when updated information is received, confirm the identity of the individual and update the information where necessary.

Principle (e) - *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.*

All special category data processed by the College for the purpose of employment or substantial public interest is retained for the periods set out in our FE Sector Retention and Disposal Schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our Retention and Disposal Schedule is reviewed periodically and updated when necessary.

The College will:

- Only keep personal data in an identifiable form as long as necessary for the purpose for which it is collected.
- Delete or pseudonymise the data once the retention period has elapsed.

Principle (f) - *Personal data shall be processed in a manner that ensures appropriate security of processing the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or Organisational measures.*

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The College implements and maintains reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data.

The College will:

- Ensure that there is the appropriate organisational and technical measures in place to protect personal data.

- Ensure staff have completed mandatory training in data protection.

4. Accountability Principle

The College will be responsible for and demonstrate its compliance with the above data protection principles by:

- Ensuring that records are kept of all personal data activities, and that these are provided to the Information Commissioner on request. The College maintains a Record of Processing Activities (Art. 30, UKGDPR) which records all of our personal data activities.
- Carrying out Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- Ensuring a Data Protection Officer is appointed to provide independent advice and monitoring of the College's personal data handling, and that this person has access to report to Senior Management.
- Having in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

5. Data Retention

Personal data is held and disposed of in line with the FE Sector Retention and Disposal Schedule. When disposing of information, the College will ensure it is destroyed securely.

6. Data Protection Officer

The DPO is the point of contact for anyone who wishes to exercise any of their data protection rights or respond to general queries. You can contact the DPO in the following ways:

Data Protection Officer
SRC Banbridge Campus
Castlewellan Road
Banbridge
Co. Down
BT32 4AY
0300 1231223
DPO@src.ac.uk

If you still have concerns, you can contact the Information Commissioner's Office (ICO) on:

Informational Commissioners Office – Northern Ireland
3rd Floor
14 Cromac Place
Belfast
BT7 2JB
0303 123 113 / 028 9027 8757

7. Related Policies and Procedures

There are a number of documents and policies relevant to Data Protection in the College:

- Data Protection Policy
- Data Subject Rights Procedure

- FE Sector Retention and Disposal Schedule
- Freedom of Information Policy
- Admissions Policy and Procedure
- Student Criminal Convictions Disclosure Policy
- Recruitment and selection Policy and Procedure
- Recruitment and employment of ex-offenders and the use of disclosure information Policy.