

# Data Protection Policy

<b>Author/Responsibility</b>	<b>Document Version</b>	<b>Date Reviewed</b>	<b>Next Review Due</b>
<b>Eoin Coyle Michelle Breslin</b>	<b>1.4</b>	<b>Jan 21</b>	<b>Jan 23</b>

## Table of Contents

Introduction .....	3
Roles and Responsibilities .....	3
The Board of Governors and Principal and Chief Executive .....	3
Data Protection Officer .....	3
Staff Responsibilities .....	4
Data Subject Responsibilities .....	4
Data Protection Principles .....	5
Lawful Basis for Processing Personal Data .....	5
Lawful Basis for Processing Special Category Data .....	6
Individuals Rights .....	6
Privacy Notices.....	7
Record of Processing Activities .....	7
Data Protection Impact Assessments (DPIAs) .....	7
As per Article 35 of the UK GDPR, the College will carry out a DPIA when processing may contain high risk privacy implications.....	7
Contracts.....	7
Consent.....	7
Disclosures to Third Parties.....	8
Disclosure to Parents (Student Information) .....	8
Disclosures to the Police.....	8
CCTV .....	8
Data Breach .....	9
Policy Awareness .....	9
Status of the Policy.....	9
Data Protection Officer contact details .....	10
Complaints and Compliments .....	10
List of Data Protection related Policies and Procedures.....	10
APPENDIX 1 Glossary of Terms .....	11
APPENDIX 2 UK GDPR Principles.....	13

## Introduction

As a Non-Departmental public authority, the College has an obligation to protect its information assets and in particular, the information relating to its employees, students and other individuals in whatever form that information is held. The College is responsible for ensuring that Personal Data is properly safeguarded and processed in accordance with Data Protection Legislation. The purpose of this policy is to set out the standards of how the College handles Personal Data whether held electronically or manually.

The College is registered as a Data Controller with the Information Commissioners Office (ICO) on an annual basis. **ICO Registration Number - Z4821243**

The College functions require us to process personal data, primarily to perform our statutory functions to deliver education and training in the Further Education sector to our students and administer contracts with our employees, workers, contractors, agency workers, consultants and suppliers and to comply with our legal obligations (for example health and safety and reporting to the Department for the Economy). Full details of what Personal Data we process, our lawful basis for processing, and what personal data is shared with third parties is as set out in the College's Privacy Notices. The College's appropriate Privacy Notice must be presented when the Data Subject first provides the Personal Data.

This policy sets out what the College expects of all its employees, workers, contractors, agency workers, consultants, directors, students, in order to comply with Data Protection legislation.

Refer to Glossary of Terms for definitions.

## Roles and Responsibilities

### [The Board of Governors and Principal and Chief Executive](#)

The Board of Governors and the Principal and Chief Executive will be responsible for raising the profile of the Data Protection Legislation. They will have ultimate responsibility for ensuring the College complies with Data Protection Legislation.

### [Data Protection Officer](#)

The position, independence and responsibility of the Data Protection Officer (DPO) has responsibility, on behalf of the Principal and Chief Executive, and as defined in Article 39 of the Regulations to:

- Inform and advise the College and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on Privacy Impact Assessments; train employees.
- Advise on Data Protection Impact Assessments and authorise before processing commences
- To raise awareness of Data Protection legislation and ensure and inform staff of relevant changes
- Conduct internal reviews

- Co-operate with the supervisory authority, the Information Commissioner's Office (ICO). To act as the contact point for the ICO on issues relating to processing, including the prior consultation referred to in Article 36
- Ensure the College is kept informed of legislative changes and that relevant amendments are implemented into the College processes.
- Ensure that employees, students and authorised third parties comply with the UK GDPR Principles (See Appendix 2), in respect of data within their remit;
- Ensure that the College Policy, guidelines and security measures are appropriate and up to date for the types of data being processed;
- Be the contact point for the administration of all Data Subject Rights relating to data held by the College.

### Staff Responsibilities

All employees, workers, directors (collectively referred to as Staff) are responsible for working in compliance with Data Protection Legislation and the conditions set out in this policy.

- Throughout the course of working with the College, Staff will have access to various extracts of Personal Data pertaining to Staff/students, depending on the nature of their role.
- Staff must adhere to all Data Protection related policies and procedures to ensure the confidentiality, integrity and availability of personal data.
- All College Staff must complete mandatory training on the UK GDPR and adhere to regular information updates on new policies and procedures as they become operational.

Compliance is the responsibility of all Staff. Any breach of this Data Protection Policy may lead to disciplinary action being taken, access to College information facilities being withdrawn, or in substantial cases, a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the DPO.

### Data Subject Responsibilities

As Data Subjects, all employees, workers, contractors, agency workers, consultants, directors, students are responsible for:

- ensuring that any personal information they provide to the College in connection with their employment, registration or other contractual agreement is accurate;
- informing the College of any changes to any personal information which they have provided, e.g. changes of address, bank details;
- responding to requests to check the accuracy of the personal information held on them and processed by the College and informing the College of any errors or changes to be made.

The College cannot be held responsible for any errors unless the data subject has informed the College of the changes.

## Data Protection Principles

The College adheres to the six principles (Article 5(1)) relating to the processing of Personal Data set out in the UK GDPR Legislation which requires Personal Data to be:

- a) Processed lawfully, fairly and in a transparent manner in relation to the data subject - (Lawfulness, Fairness and transparency)
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes – (Purpose limitation)
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89\(1\)](#) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject – (Storage Limitation)
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

Article 5(2) of the UK GDPR legislation requires that:

The Controller shall be responsible for, and be **able to demonstrate** compliance with the Data Protection Principles listed above.

### [Lawful Basis for Processing Personal Data](#)

You may only collect, process and share Personal Data fairly and lawfully and for specified purposes.

The College will ensure all processing is affiliated to one or more of the following:

- a) Consent: the Data Subject has given clear consent to process their personal data for a specific purpose.
- b) Contract: the processing is necessary for purposes of a contract with the Data Subject, or with a view to entering into a contract.
- c) Legal obligation: the processing is necessary to comply with legislation (not including contractual obligations).
- d) Vital interests: the processing is necessary to protect someone's life.
- e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- f) Legitimate interests: the processing is necessary for legitimate interests or 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 cannot apply if you are a public authority processing data to perform official tasks.) Where the College relies on Legitimate Interest as a lawful basis, a Legitimate Interest Assessment (LIA) will be carried out.

### Lawful Basis for Processing Special Category Data

- a) explicit consent – consent which can be demonstrated
- b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- c) processing is carried out in the course of its legitimate activities with appropriate safeguards
- d) processing relates to personal data which are manifestly made public by the data subject
- e) processing is necessary for the establishment, exercise or defence of legal claims
- f) processing is necessary for reasons of substantial public interest
- g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems
- h) processing is necessary for reasons of public interest in the area of public health
- i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

## Individuals Rights

Data Protection Legislation provides the following rights for individuals which the College will respond to within the provision of the law. These rights are not absolute.

The right to receive certain information about our Processing activities

- 1) The right of access to Personal Data
- 2) The right to rectification of inaccurate or incomplete data
- 3) The right to ask us to erase their Personal Data if it no longer necessary in relation the purposes for which it was collected or processed
- 4) The right to restrict processing in certain specific circumstances
- 5) The right to data portability in certain specific circumstances
- 6) The right to object in certain specific circumstances (for example to us processing for direct marketing purposes)

- 7) Rights in relation to automated decision making and profiling
- 8) Right to Withdraw Consent
- 9) Right to Complain to the Information Commissioners Office (ICO)

All requests made in relation to the rights listed above should immediately be forwarded to the DPO. Further information in this regard can be found in the '**Data Subject Rights Procedure**'.

## **Privacy Notices**

As per Article 13 of the UK GDPR, the College will provide Privacy Notices on College websites and points of data collection to inform Data Subjects of how their data will be used.

## **Record of Processing Activities**

As per Article 30 of UK GDPR, the College will maintain a record of processing activities.

## **Data Protection Impact Assessments (DPIAs)**

As per Article 35 of the UK GDPR, the College will carry out a DPIA when processing may contain high risk privacy implications

## **Contracts**

Data Controllers and Data Processors are both liable in the event of a data breach therefore individuals and departments who enter into a contract with a third party data processor are responsible for ensuring that all processing of personal data carried out on behalf of the College is done in compliance with this policy and related procedures. Further guidance is available in the 'Data Protection Handbook'. In the absence of a contract, the Director/Head of Department must ensure there is a Data Sharing Agreement (DSA) in place.

## **Consent**

Data Subjects are able to withdraw consent, therefore it is the College Policy that consent should only be relied on as the lawful basis for processing in exceptional circumstances. Where the College relies on consent as a condition for processing, it will:

- Ensure the consent is clear and unambiguous (e.g. no pre-ticked opt-in boxes)
- Place consent declarations separate from other associated terms and conditions that may exist
- Provide clear and easy ways for subjects to withdraw consent at any time including contact details of a responsible owner
- Act on withdrawals of consent as soon as possible
- Retain records of consent/withdrawals of consent throughout the lifetime of the data processing.

The DPO must be contacted to ensure:

- consent is the appropriate legal basis for the processing in question
- obtaining of consent meets the requirements of the Data Protection Legislation
- open transparency to the data subjects.

Further guidance is available in the 'Data Protection Handbook'.

## **Disclosures to Third Parties**

Personal Data will not be shared with third parties unless certain safeguards or contractual arrangements are in place or where there is a legal or statutory obligation to disclose.

In dealing with a request the College will be sensitive to and give proper consideration to the data subjects rights and privacy in relation to any 'third party' information contained in the response. Personal data will only be disclosed to a third party where a lawful basis exists.

Special Category personal data will only be disclosed or collected where a lawful basis specific to Special Category data, as defined by Data Protection Legislation, is met.

Personal data will only be disclosed outside of the EEA (the EU Member States together with Iceland, Liechtenstein and Norway) where additional conditions as defined by Data Protection Legislation are met.

Further guidance is available in the 'Data Protection Handbook'.

### [Disclosure to Parents \(Student Information\)](#)

The College will not disclose Personal Data of students to parents or next of kin where we have no consent from the student to do so. There may be exceptional circumstances to this rule, for example where it necessary to protect the vital interest of student or someone else.

Guidance in relation to the disclosure of personal data to parents or guardians about their son or daughter is provided in the College's Safeguarding Policy & Procedures.

### [Disclosures to the Police](#)

In certain circumstances the College will be able to disclose Personal Data to the police for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders.

Further guidance is available in the 'Data Protection Handbook'.

## **CCTV**

All employees, students and visitors should have a reasonable expectation of being captured on CCTV on a daily basis.

While the use of CCTV is primarily for the following purposes, the College will regulate its use within the provisions of Data Protection Legislation so as not to



become intrusive:

- Deterring, prevention and detection of a crime including misuse/abuse of College equipment.
- Identification, apprehension and prosecution of offenders.
- Security of campus buildings and ground.
- Safeguarding/Health and Safety

In some circumstances the images may be viewed for investigatory purposes.

## **Data Breach**

In the event of an actual, suspected or potential breach, the College will take immediate action to secure the information and mitigate any further or possible compromise of data.

If a data security breach occurs, the College will respond to and manage the breach effectively by means of a 5 part process.

- 1) Reporting a Breach
- 2) Containment and Recovery
- 3) Assessing the Risks
- 4) Notification of Breaches
- 5) Evaluation and Response

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately and without delay contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

Suspected or confirmed breaches which may cause damage/distress to the data subjects must be reported to the ICO within 72 hours by the DPO, from when the College becomes aware of it. In the event of a sufficiently serious data breach, the College will notify the public or associated personnel without undue delay.

You can email [databreach@nwrc.ac.uk](mailto:databreach@nwrc.ac.uk)

## **Policy Awareness**

Data Protection awareness is a mandatory element of all employee induction. Policies and procedures will be circulated to all employees and published on the College Intranet/Internet for employees, students and members of the public to view. All employees, workers, contractors, agency workers, consultants, directors, students are required to be familiar with and comply with the policy at all times.

## **Status of the Policy**

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time.


Failure to comply with this policy may result in damage to College reputation, data loss, damage and distress to the individuals affected and may lead to disciplinary action.

## Data Protection Officer contact details

The DPO is the point of contact for anyone who wishes to exercise any of the Rights as listed above or respond to general queries. You can either write to or email on:

 **Data Protection Officer**  
**Eoin Coyle**

**NWRC**  
**Strand Road**  
**Derry~Londonderry**  
**BT48 7AL**

 **02871 276154**

 [dpo@nwrc.ac.uk](mailto:dpo@nwrc.ac.uk)

 [databreach@nwrc.ac.uk](mailto:databreach@nwrc.ac.uk)

## Complaints and Compliments

Individuals concerned about any aspect of the management of personal data at the College may raise their concerns by following the FE Sector Complaints and Compliments Procedure available via [www.nwrc.ac.uk/policies](http://www.nwrc.ac.uk/policies) .

## List of Data Protection related Policies and Procedures

There are a number of documents and policies relevant to Data Protection. It is recommended that all documentation is reviewed to ensure a comprehensive understanding of Data Protection Legislation and how it applies to the College.

- Data Breach Management Procedure
- Data in Transit Policy
- Data Protection Handbook
- Data Protection Privacy Notice
- Data Subjects Rights Procedure
- Retention and Disposal Schedule Policy
- Store Procedure
- Clear Desk Policy
- Code of Practice – IT Services & MIS Personnel
- Freedom of Information Policy
- Freedom of Information Act Publication Scheme
- Freedom of Information Guide for Applicants
- Freedom of Information Disclosure Guidelines
- Freedom of Information Request Form
- Freedom of Information Charging Fees

## APPENDIX 1 Glossary of Terms

### Consent

- any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

### Data Breach

- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

### Data Controller

- the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

### Data Processor

a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

### Data Protection Impact Assessments (DPIAs)

- process designed to allow organisations to systematically analyse, identify and minimise the data protection risks of a project or plan. DPIAs are a legal requirement for any type of processing that is likely to result in a high risk to the rights and freedoms of individuals

### Data Subject

- **Data subject** means an individual who is the **subject** of personal **data**.

### Information Asset

- A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

### Information Commissioner's Office (ICO)

- The ICO is the supervisory and regulatory authority responsible for upholding individuals' rights and ensuring all Data Controllers process personal data within the provisions of legislation.

### Personal Data

- any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Privacy Notice

- a public document from an organisation that explains how that organisation will process personal data and how it applies the data protection principles. A privacy notice will provide information on the identity and contact details of the controller, contact details of the DPO, purposes of processing, recipients or categories of recipients and if the controller intends to transfer personal data to a third country or organisation.

## Process, Processing and Processed

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

## Record of Processing Activities


- an internal record of an organisations processing activities relating to personal data which contains, name of the controller, purposes of processing, description of the categories of data subjects and categories of personal data, recipients, where applicable transfers to third countries or international organisations, time limits of erasure and a general description of the technical and organisational security measures.

## Special Category Data

- personal data revealing 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

The ICO contact details are:

 **Information Commissioner's Office – Northern Ireland**  
**3<sup>rd</sup> Floor**  
**14 Cromac Place**  
**Belfast**  
**BT7 2JB**

 **Tel: 0303 123 1113 or 028 9027 8757**

## Third Party

- a natural or legal person, public authority, agency or body **other** than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

## APPENDIX 2 UK GDPR Principles

Article 5(1) of the UK GDPR requires that personal data shall be:

**1) *Processed lawfully, fairly and in a transparent manner in relation to the data subject - (transparency)***

The first UK GDPR principle states that personal data must be processed fairly and lawfully. As a means to demonstrate fairness, the College will actively communicate our processing activities to data subjects. This will be visible by means of Privacy Notices, Privacy Impact Assessments (PIA's), website information and information updates if there is an unforeseen change to how we use personal data. Communications will be concise, easily accessible and written in clear and plain language. This commitment will be compliant with Articles 13 and 14 of UK GDPR.

**2) *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes – (Purpose limitation)***

The second principle of UK GDPR signifies the Colleges responsibility to only use information for the purposes for which it was provided.

**3) *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)***

The third principle of UK GDPR means the College will not ask for more information than is necessary to conduct its overall business and statutory obligations. The College may process personal data for the purposes of Public interest, or scientific/historical/research/statistical purposes however consideration will be paid to safeguarding the rights and freedoms of the data subjects

**4) *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)***

The fourth Principle places responsibility on the College to ensure the integrity and accuracy of its data. Employees must ensure a high level of accuracy when inputting personal data onto any system. Data is only valuable and decisions accurate where the information is correct and up to date. Each data subject has a responsibility to inform the College of any changes to their personal information for records to be updated. The College cannot be held accountable if it receives data which is inaccurate.

**5) *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are***

***processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89\(1\)](#) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject – (Storage Limitation)***

The fifth principle relates to storage limitation and the College responsibility to archive or dispose of data in line with the FE Sector Retention and Disposal Schedule. The College will not keep information for longer than is necessary with the exemption of Public interest, or scientific/historical/research/statistical purposes. Personal Data that is no longer needed for specified purposes, should be deleted or anonymised.

***6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)***

The sixth principle places responsibility on all employees, students and any third parties authorised to access the College's personal data sets to ensure that those data, whether held electronically or manually, are kept secure and not disclosed or processed unlawfully, in accordance with UK GDPR.

Article 5(2) of the UK GDPR requires that:

***a) The controller shall be responsible for, and be able to demonstrate compliance with the data protection principles listed above.***

The College will demonstrate compliance with the above principles by means of both appropriate organisational and technical measures. These measures may include relevant policies and standard operating procedures, Privacy Impact Assessments (PIA's), Privacy Notices, internal reviews, staff training, awareness campaigns and the appointment of a DPO.