Data Protection Policy

SECTOR POLICY

Version 6

Scope of Policy:	All Staff and Students
Policy Owner:	Head of Corporate Development
Date Approved:	25/05/2022
Approved By:	Strategic Leadership Team
Status:	Current
Publication Date:	06/01/2026
Equality Screening Date:	08/03/2018
Policy Review Date:	17/10/2027

Published by Belfast Metropolitan College www.belfastmet.ac.uk. Belfast Metropolitan College ['Belfast Met'] is committed to providing publications that are accessible to all. To request additional copies of this publication in a different format please contact:

Corporate Development
Belfast Metropolitan College
Integrated Shared Services Centre
398 Springfield Road
Belfast. BT12 7DU

This document is only valid on the day it was printed. The master and control version of this document will remain with Corporate Development. Amended and approved versions of the policy must be sent to Corporate Development once approved. Final versions will be posted on the intranet by Corporate Development.

Further Information
For further information about the content of this policy please contact:

Corporate Development
Belfast Metropolitan College
Integrated Shared Services Centre
398 Springfield Road
Belfast. BT12 7DU

Policy Compliance details:-

Compliance with Equality Legislation.

PLEASE NOTE: Policies must be equality screened before being submitted to SLT and Trade Unions:-

Equality Screening Date:	08/03/2018
Equality Screening Outcome:	Screened Out
Sector or Local Screening:	Local Screening
Consultation Date (if applicable):	Not Applicable
Equality Impact Assessment	Not Applicable
(EQIA) Date (if applicable):	Not Applicable
EQIA Key Outcomes:	Not applicable

Document History

Version Number	Author	Amendments/Updates	Date
1.0	Finance Department	Sector changes	2013
1.1	Finance Department	Sector changes	2015
1.2	Finance Department	Sector Changes	2016
2.0	Corporate Development	Redrafted by the Sector to give effect to the New General Data Protection Legislation effective from 25th May 2018. Changes made throughout policy to reflect the impact of the new Data Protection Principles, roles and responsibilities. Most significant changes around lawful processing and sharing information, disclosure of information, individuals rights and consent.	Nov 2018
3.0	Corporate Development	Updated by the Sector to include new definitions into the Glossary	July 2019
4.0	Corporate Development	Changes implemented following UK GDPR. References to GDPR changed to UK GDPR. Paragraph 1 first sentence to summarise all those whose information is protected. Paragraph 3 to reflect a separation of roles between the DPO and the Data Protection and Complaints Officer. Director of People and Place changed to Director of People. Changes from DPO to Data Protection and Complaints Officer throughout the Policy. Paragraph 6 Additional section to provide details about how to make a Subject Access Request (SAR). Additional Paragraphs at 7, 8 and 9 as agreed with the Sector. Changes to paragraphs 10, 11 and 12 to clarify the location of the Data Protection Handbook. Paragraph 12, third section changed to reflect the changes post Brexit. Paragraph 13, CCTV Policy referenced. Paragraph 18 – complaints section added.	March 2022

		Paragraph 19 – linking supporting documents referenced.	
4	Corporate Development	Paragraph 3 changed from Gillian Magee, Director of People to Aidan Sloane, Chief Operating Officer	June 2023
4	Corporate Development	Change Data Protection and Complaints Officer to Data Protection and Complaints Executive. Paragraph 3 - Change contact details of DPO from Aidan Sloane Chief Operating Officer, to Elaine McElhill Data Protection Officer and Compliance Manager	9 November 2023
5.0	Corporate Development	Localised policy updates: Section 4 – Lawful Basis for Processing Special Category Data and Criminal Offence Data - Description of Special Category Data specified. New Section 4, Subsection added - 'Criminal Offence Data' - a requirement from an OU Audit 2023-24 to describe the College's lawful basis to process Criminal Offence Data. New Section 4 subsection added - 'Appropriate Policy Document (APD)' - OU Audit 2023-24 recommendation. Section 12 - Disclosures to Third Parties Subsection update - 'Disclosures to the Police' - inclusion of narrative referring to PSNI requests/Form 81s.	26 February 2024
6.0	Corporate Development	Updated contact details, and small wording and formatting changes throughout the document ICO registration number updated 11.2 Disclosures to Policy updated to provide clarity on process 13 Data Breach updated to provide clarity on process and reference to Data Breach Management Procedure 18 Supporting Documents list refine 19 Review added detailing that the Policy will be reviewed at least every two years.	17 October 2025

6.1	Corporate Development	Formatting corrections and update to external document links where required	6 January 2026

Table of changes made to a policy, by whom and when

Distribution

This document has been distributed as follows:

Name	Date (where applicable)
Trade Union	N/A
Strategic Leadership Team	9 November 2018; 26 May 2022
ARAC Committee	N/A
Governing Body	N/A
Published on intranet/website by Corporate Development	12 November 2018; 26 May 2022; June 2023; Feb 2024; October 2025; January 2026

Table of who has seen the policy and when

Contents

1. Background/Introduction

As a public authority, Belfast Metropolitan College (the College) has an obligation to protect its information assets and, in particular, the information relating to its employees, workers, 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 the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (collectively referred to in this document as Data Protection Legislation).

The College is registered as a Data Controller with the Information Commissioners Office (ICO) on an annual basis**.** Belfast Metropolitan College's Registration number is ZB046129.

The College's functions require the process of personal data, primarily to perform statutory functions. This is required in order to deliver education and training to our students in the Further Education sector, to administer contracts with employees, workers, contractors, agency workers, consultants and suppliers, and to comply with legal obligations (for example health and safety and reporting to the Department for the Economy).

Full details of the personal data processed, lawful basis for processing, and what personal data is shared with third parties is as set out in the College's Privacy Notices. The appropriate College Privacy Notice must be presented before 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, and students, in order to comply with current Data Protection legislation.

An associated Glossary of Terms is provided in **Appendix 1**.

2. Aim

The purpose of this policy is to set out the standards of how the College handles personal data, whether held electronically or manually.

3. Roles and Responsibilities

3.1 The Board of Governors and Principal and Chief Executive

The Board of Governors and Principal and Chief Executive will endorse and support in assisting in raising the profile of the Data Protection legislation. They will have ultimate responsibility for ensuring the College complies with all data protection legislation.

3.2 Data Protection Officer

The College's registered Data Protection Officer (DPO) has responsibility, on behalf of the Principal and Chief Executive, for the duties defined in Article 39 of the Data Protection Legislation.

The College's Data Protection and Complaints Executive currently undertakes the following duties, as set out in Article 39 of the UK GDPR, on behalf of the registered DPO:

- Inform and advise the College and its employees about their obligations to comply with the Data Protection Legislation and other data protection laws.
- Monitor compliance with the Data Protection legislation and other data protection laws, including managing internal data protection activities, advice on Privacy Impact Assessments; train employees and conduct internal audits.
- Cooperate with the supervisory authority, the Information Commissioner's Office (ICO).
- Act as the contact point for the ICO on issues relating to processing, including the prior consultation referred to in Article 39.
- 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 Data Protection legislation principles 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 subject access requests relating to data held by the College.

3.3 Staff Responsibilities

All employees, workers, contractors, agency workers, consultants, 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 Data Protection legislation and adhere to regular information updates on new policies and procedures as they become operational.

3.4 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; and

- 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.

4. UK GDPR Principles

The College adheres to the six principles of Data Protection as set out in Article 5(1) of the legislation (see Appendix 2), which refers to the processing of Personal Data. This data must 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 Data Protection Legislation requires that:

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

4.1 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.

4.2 Lawful Basis for Processing Special Category Data and Criminal Offence Data

Special Category Data

Special Category Data can be defined at Article 9 of the UK GDPR as personal information of data subjects that is especially sensitive, the exposure of which could significantly impact the rights and freedoms of data subjects and potentially be used against them for unlawful discrimination.

Special Category data is a follows:

- Racial or ethnic origin
- Political Opinions
- Religious of Philosophical beliefs
- Trade Union Membership
- 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.
- Criminal Offence Data

Criminal Offence Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 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".

You may only process special category data and criminal offence data if you identify both a lawful basis for general processing and an additional condition for processing this type of data, the additional conditions being affiliated to one or more of the following:

a. Explicit consent — consent that 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 that 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 preventative 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.

4.3 Appropriate Policy Document (APD)

As the College processes special category and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018, we are required to have in place an APD and publish on the College website with College Privacy Notices.

The College processes special category data about our students and employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union.

The College is permitted to process criminal convictions and offences data as well as undertaking mandatory criminal record checks to carry out our obligations in respect of its public task, and to comply with its legal obligations, including: employment, social security and social protections, preventing or detecting unlawful acts, protecting the public against dishonesty and safeguarding of children and individuals at risk.

The policy provides information about the safeguards that the College has put in place in accordance with the Data Protection principles.

The College's retention and disposal practices are set out in the Retention and Disposal Schedule.

Further information can be found in the Data Protection section on the staff intranet.

5. Individuals Rights

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

These include:

1. The right to receive certain information about College Processing activities.

2. The right of access to personal data.
3. The right to rectification of inaccurate or incomplete data.
4. The right to ask us to erase their personal data if it is no longer necessary in relation the purposes for which it was collected or processed.
5. The right to restrict processing in certain specific circumstances.
6. The right to data portability in certain specific circumstances.
7. The right to object in certain specific circumstances (for example, to our processing for direct marking purposes).
8. Rights in relation to automated decision making and profiling.
9. Right to withdraw consent.
10. Right to complain to the Information Commissioner's Office (ICO).

All requests made in relation to the rights listed above should immediately be forwarded to the College's Data Protection and Complaints Team by emailing dataprotection@belfastmet.ac.uk, who will provide advice and assistance on responding to the request.

Further information in this regard can be found in the 'Data Subject Rights Procedure' located in the Data Protection section of the staff intranet.

5.1 Requests by Data Subjects

Data subjects have a right to access their personal data. Requests can be made in the following ways:

Complete the data subject rights form on our website.

Email dataprotection@belfastmet.ac.uk.

6. Privacy Notices

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 about how their data will be used.

7. Recording of Processing Activities

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

8. Data Protection Impact Assessments (DPIAs)

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

9. 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. Further guidance is available for staff in the 'Data Protection Handbook' located in the Data Protection section of the staff intranet. In the absence of a contract, the Head of Department or Director must ensure that there is a Data Sharing Agreement (DSA) in place.

10. Consent

Data Subjects are able to withdraw consent; therefore, it is 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 terms and conditions.
- 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 Data Protection and Complaints Team (dataprotection@belfastmet.ac.uk) is able to provide guidance to ensure that:

- Consent is the appropriate legal basis for the processing in question.
- The obtaining of consent meets the requirements of Data Protection Legislation.
- All information is open and transparent to the data subjects.

Further guidance is available in for staff in the 'Data Protection Handbook' located in the Data Protection section of the staff intranet.

11. 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 where a lawful basis specific to Special Category data, as defined by Data Protection Legislation, is met.

Personal data will only be disclosed outside to countries outside the UK when it is lawful to do so i.e. if an adequacy decision is in place or where additional conditions as defined by Data Protection Legislation are met.

Further guidance is available for staff in the 'Data Protection Handbook' located in the Data Protection section of the staff intranet.

11.1 Disclosure to Parents (Student Information)

The College will not disclose the 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 is necessary to protect the vital interest of the student or of someone else.

Guidance in relation to the disclosure of personal data to parents or guardians about persons in their care is provided in the Safeguarding, Care and Welfare Policy, which is located on Public Documents page of the Belfast Met's website.

11.2 Disclosures to the Police

In certain circumstances, the College may be able to disclose personal data to the police for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders.

On receipt of a request from the police for personal data, contact the Data Protection & Complaints Team (dataprotection@belfastmet.ac.uk) who will provide guidance and assistance on responding to the request.

12. CCTV

All employees, students and visitors should have a reasonable expectation of being captured on CCTV on a daily basis. There are signs on each campus to alert all employees, students and visitors that CCTV imagery is being used.

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 exceptional circumstances, the images may be viewed for investigatory purposes. The College's CCTV Policy provides further details.

13. 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 way of a five-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 Data Protection and Complaints Team (dataprotection@belfastmet.ac.uk or use the contact details noted in Section 16). You should preserve all evidence relating to the potential personal data breach.

The Data Protection & Complaints Team will assess the associated risks and advise as to whether notifications to the ICO and/or impacted individuals are required. Further information is available in the Data Breach Management Procedure.

14. Policy Awareness

Data Protection legislation awareness is a mandatory element of all employee induction and is rolled out to existing staff on an annual basis. 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 staff and students are required to be familiar with and comply with the policy at all times.

15. 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.

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

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 addressed initially with the Data Protection and Complaints Executive.

16. Data Protection Contact Details

The Data Protection and Complaints Team 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 them on:

Data Protection
Belfast Metropolitan College
Corporate Development
Integrated Shared Services Centre
398 Springfield Road
Belfast, BT6 7DU

dataprotection@belfastmet.ac.uk
02890 265455

Contact details for the **Information Commissioner's Office** (ICO) are as follows:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113 or 01625 545 745

17. Complaints

Any complaints regarding the operation of this policy should be made in the first instance to:-

Complaints
Belfast Metropolitan College
Corporate Development
Integrated Shared Services Centre
398 Springfield Road
Belfast, BT6 7DU

complaints@belfastmet.ac.uk
02890 265455

If you are not satisfied with the way in which your complaint has been handled, you have the right to complain to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113 or 01625 545 745

Or the Public Services Ombudsman:-

Northern Ireland Public Services Ombudsman
Progressive House
33 Wellington Place
Belfast BT1 6H

18. Data Protection Policies supporting documents

This policy is supported by the following supporting documents:-

- Data Protection Handbook (staff)
- Data Subject Rights Procedure (staff)
- Data Subject Rights Request
- Data Breach Management Procedure
- Data Breach Reporting Form
- Data Sharing Agreement Templates
- FE Sector Retention and Disposal Schedule

19. Review

This Policy will be reviewed (and amended if necessary) every two years, or sooner if required to reflect changes in legislation or circumstances.

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 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.

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.

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.

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 its 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 audits, staff training, awareness campaigns and the appointment of a DPO.