# POLICIES & PROCEDURES

# DATA PROTECTION POLICY (UK GDPR)

| | |
|---|---|
| **Policy Owner:** | Data Protection Officer |
| **Date Approved:** | 04 November 2026 |
| **Version:** | V4.1 |
| **Equality Screening Date:** | 11 August 2026 |
| **Date of First Issue:** | 13 June 2018 |
| **Date of Next Review:** | October 2028 |
| **Location:** | Gateway and SWC Website |

# CONTENTS


1. Introduction....2
2. Policy Purpose and scope....2
3. Roles and Responsibilities....3
4. Data Protection Principles....5
5. Lawful Basis for Processing Personal Data....6
6. Lawful Basis for Processing Special Category Data....6
7. Lawful Basis for Processing Criminal Offence Data....8
8. Individuals Rights....8
9. Data Protection Complaints....9
10. Privacy Notices....10
11. Record of Processing Activities....10
12. Data Protection Impact Assessments (DPIAs)....10
13. Contracts....11
14. Consent....11
15. Disclosures....12
16. CCTV....13
17. Data Breach....13
18. Policy Awareness....14
19. Status of the Policy....14
20. Data Protection Officer contact details....14
21. Policy Review....15

Appendix 1: Glossary of Terms....16
Appendix 2: UK GDPR Principles....18
Related Documentation....21
Change Log....21
Communication....21
Document Development....21
Approval Dates....21
Document History....22

## 1. Introduction

1.1 As a Non-Departmental Public Body, 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 the United Kingdom General Data Protection Regulations (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, (collectively referred to in this document as Data Protection Legislation).

1.2 The College is registered as a Data Controller with the Information Commissioners Office (ICO) on an annual basis with registration number, Z1124639.

1.3 The College functions require us to process personal data, primarily to perform our statutory functions to deliver education and training in the Further and Higher Education sector to all our students; and to 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).

1.4 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 Privacy Notice must be brought to the attention of the Data Subject when they first provide the Personal Data e.g., enrolment or application form. Privacy Notices can be found on the College website.

1.5 A definition of terms used in this policy can be viewed in Appendix 1 Glossary of Terms.

## 2. Policy Purpose and scope

2.1 The purpose of this policy is twofold:

(i) To set out the standards for the handling of Personal Data whether held

electronically or manually by South West College "the College".

(ii) To set out what the College expects of its Governing Body, and all employees, workers, contractors, agency workers, consultants, students; in order to comply with Data Protection Legislation.

## 3. Roles and Responsibilities

### 3.1 The Board of Governors and Principal and Chief Executive

3.1.1 The Board of Governors and Principal and Chief Executive will endorse and support this policy in assisting the raising of the profile of the Data Protection Legislation within the college. They will have ultimate responsibility for ensuring the College complies with Data Protection Legislation.

### 3.2 Data Protection Officer

3.2.1 The Data Protection Officer (DPO) has responsibility, on behalf of the 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 UK GDPR and other data protection laws.
- Monitor compliance with UK GDPR and other data protection laws, including managing internal data protection activities, advise on Privacy Impact Assessments; train employees and conduct internal audits.
- Co-operate 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 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, 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

3.3.1 All governors, 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.

3.3.2 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. Therefore:

- 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 UK GDPR and adhere to regular information updates on new policies and procedures as they become operational.
- Staff must not make unauthorised disclosures of personal data.
- Staff must immediately notify the Data Protection Officer (DPO) of any breaches they are aware of.
- Staff must not breach 'Data Protection Principles'.

3.3.3 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.

## 3.4 Data Subject Responsibilities

3.4.1 As Data Subjects, all governors, 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, enrolment 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.

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

## 4. Data Protection Principles

4.1 The College adheres to the six principles (Article 5(1)) relating to the processing of Personal Data set out in the UK GDPR and the Data Protection Act 2018 which requires Personal Data to be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (*Lawfulness, Fairness and Transparency).*
- 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*).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*Data Minimisation*).
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*Accuracy*).
- 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. The College adheres to the 'FE Retention and Disposal Schedule' (*Storage Limitation).*
- 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*).

4.2 Article 5(2) of the GDPR requires that the controller shall be responsible for, **and be able to demonstrate** compliance with, the Data Protection Principles listed above.

## 5. Lawful Basis for Processing Personal Data

5.1 The College may **only** collect, process, and share Personal Data fairly and lawfully and for specified purposes.

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

- **Consent:** the Data Subject has given clear consent to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for purposes of a contract with the Data Subject, or with a view to entering into a contract.
- **Legal obligation:** the processing is necessary to comply with legislation (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 for official functions, and the task or function has a clear basis in law.
- **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. (Note - This cannot apply if we are a public authority processing data to perform official tasks.)

## 6. Lawful Basis for Processing Special Category Data

6.1 The College is required to process special category data which is 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 freedom of

data subjects and potentially be used against them for unlawful discrimination.

Special Category data is as 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;
- Data concerning a natural person's sex life or sexual orientation; or
- Criminal Offence Data.

6.2 The College will only process special category data if one of the following applies:

- Explicit consent has been given by the data subject i.e. consent which can be demonstrated.
- 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.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- 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.
- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

## 7. Lawful Basis for Processing Criminal Offence Data

7.1 The College may process personal data relating to criminal convictions, offences, alleged offences and related security measures where permitted by Article 10 UK GDPR and the Data Protection Act 2018. Such processing will only be undertaken where a lawful basis exists and an appropriate condition under Schedule 1 of the Data Protection Act 2018 is satisfied.

## 8. Individuals Rights

8.1 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.
- The right of access to Personal Data.
- The right to rectification of inaccurate or incomplete data.
- The right to ask us to erase their Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed.
- The right to restrict processing in certain specific circumstances.
- The right to data portability in certain specific circumstances.
- The right to object in certain specific circumstances (for example to use processing for direct marking purposes).
- Rights in relation to automated decision making and profiling.
- Right to withdraw consent.
- Right to Complain to the Information Commissioners Office (ICO).

8.2 Individuals may exercise their rights under Data Protection Legislation by submitting a request to the College. Requests may be made in writing, by email, or through any designated form or process published by the College.

8.3 Requests relating to the right of access, rectification, erasure, restriction of processing, objection, data portability, withdrawal of consent, or any other data subject right should be directed to the Data Protection Officer at gdpr@swc.ac.uk.

8.4 The College may seek proof of identity before responding to a request and will respond within the timescales prescribed by Data Protection Legislation.

8.5 Further information regarding the exercise of individual rights can be found in the College's 'Data Subject Rights Procedure'.

## 9. Data Protection Complaints

9.1 This Policy is informed by evolving legislative requirements, including the Data (Use and Access) Act 2025, and reflects the College's commitment to accountability and transparency in the handling of Personal Data.

9.2 The College is committed to ensuring that all Personal Data are processed in accordance with Data Protection Legislation and in a fair and transparent manner.

9.3 The College will take all data protection complaints seriously and will ensure that they are handled promptly, fairly and consistently.

9.4 Any individual who is dissatisfied with how the College has processed their Personal Data, or how it has responded to a request under Data Protection Legislation, has the right to raise a complaint.

9.5 Complaints may be received from data subjects, staff, students or third parties and should be directed in the first instance to the Data Protection Officer (DPO) at gdpr@swc.ac.uk.

9.6 Upon receipt of a complaint, the College will:

- Acknowledge receipt of the complaint within 30 calendar days;
- Record the complaint and any supporting information;
- Undertake a proportionate investigation into the matters raised without undue delay;
- Keep the complainant informed of progress where appropriate;
- Seek to resolve the complaint, including the implementation of any appropriate remedial actions;

- Provide the complainant with the outcome of the complaint without undue delay.

9.7 The DPO will oversee the handling of all data protection complaints and will act as the primary point of contact for the complainant.

9.8 Where appropriate, the College will use the outcome of complaints to inform improvements to its policies, procedures and staff training.

9.9 Raising a complaint under this section does not affect the individual's right to raise a concern with the Information Commissioner's Office (ICO). Individuals will be advised of their right to escalate the matter to the ICO where they remain dissatisfied with the outcome of the College's response.

## 10. Privacy Notices

10.1 The College will provide Privacy Notices on its website and when data is collected as per Article 13 of the GDPR. These Privacy Notices will inform data subjects inter alia of how their data will be used, why it is needed, and who it may be shared with. The Privacy Notices will be reviewed regularly.

## 11. Record of Processing Activities

11.1 The College will maintain a record of processing activities in line with Article 30 of the GDPR.

## 12. Data Protection Impact Assessments (DPIAs)

12.1 The College will undertake a DPIA when required by Article 35 of the GDPR and as a matter of good practice.

## 13. Contracts

13.1 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 in the 'UK GDPR Handbook'. In the absence of a contract, senior managers must ensure that there is a Data Sharing Agreement (DSA) or a Data Processing Agreement (DPA) in place as appropriate.

## 14. Consent

14.1 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 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.

14.2 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 UK GDPR.
- Open transparency to the data subjects.

Further guidance is available in the 'UK GDPR Handbook'.

## 15. Disclosures

### 15.1 Disclosures to Third Parties

15.1.1 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.

15.1.2 In dealing with a subject access request or data request the College will be sensitive to and give proper consideration to the data subject's rights, as well as the rights in relation to any other individual whose information or data is contained in the data requested 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.

15.1.3 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.

15.1.4 Personal data will only be disclosed to countries outside of 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.

15.1.5 Further guidance is available in the 'UK GDPR Handbook'.

### 15.2 Disclosure to Parents (Student Information)

15.2.1 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 the student or someone else.

### 15.3 Disclosures to the Police

15.3.1 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, the apprehension or prosecution of offenders. All requests from the Police Service of Northern Ireland (PSNI) or other law enforcement agencies should be referred to the DPO before any disclosure is made.

15.3.2 Further guidance is available in the 'UK GDPR Handbook'.

## 16. CCTV

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

16.2 While the use of CCTV is primarily for the following purposes, the College will regulate its use within the provisions of UK GDPR 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 grounds.
- Safeguarding/Health and Safety.
- Disciplinary Procedures.
- Insurance.
- Legal Proceedings.

16.3 In exceptional circumstances, the images may be viewed for investigatory purposes.

## 17. Data Breach

17.1 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.

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

(i) Reporting a breach.
(ii) Containment and recovery.
(iii) Assessing the risks.
(iv) Notification of breaches.

(v) Evaluation and Response

17.3 Any member of Staff becoming aware, or suspect, that a Personal Data Breach has occurred, should not attempt to investigate the matter but immediately, and without delay, contact the DPO. All evidence relating to the potential Personal Data Breach should be preserved.

17.4 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 without undue delay.

## 18. Policy Awareness

18.1 GDPR 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 this policy at all times.

## 19. Status of the Policy

19.1 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.

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

## 20. Data Protection Officer contact details

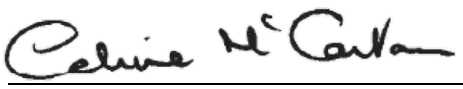
20.1 The DPO is the point of contact for anyone who wishes to exercise any of the rights

as listed above or respond to general queries. The Data Protection Officer is **Nicola Nugent**. You can either write to or email on:

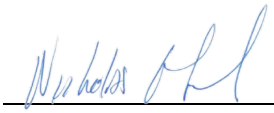
Data Protection Officer
South West College, 2 Mountjoy Road, Omagh, Co Tyrone BT79 7AH
Telephone: 028 82250109 or Ext 5231 Email: gdpr@swc.ac.uk

## 21. Policy Review

21.1 The College will ensure that adequate resources are made available to promote this policy effectively with staff and it is committed to this policy being reviewed every 2 years.

Signed Principal and Chief Executive: 

Date: 04 November 2026

Signed Chair of the Governing Body: 

Date: 04 November 2026

## 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 UK GDPR, the controller or the specific criteria for its nomination may be provided for by UK GDPR.

**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. The ICO contact details are:

**Information Commissioner's Office**
**Wycliffe House**
**Water Lane**
**Wilmslow Cheshire SK9 5AF**

**Tel: 0303 123 1113 or 01625 545 745**

**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 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 (PIAs), 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 College's 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 or data not kept up to date.

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 (Link to 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 (PIAs), Privacy Notices, internal audits, staff training, awareness campaigns and the appointment of a DPO.

**Related Documentation**

| Title | Location | Owner |
|---|---|---|
| Access to Information Policy | Gateway<br>SWC website | Data Protection Officer |
| GDPR Staff Handbook | Gateway | Sector/Data Protection Officer |
| FE Retention and Disposal Schedule | Gateway<br>SWC website | Sector/Data Protection Officer |
| Data Breach Management Procedure | Gateway | Sector/Data Protection Officer |
| Data Subject Rights Procedure | Gateway | Data Protection Officer |
| CCTV Policy | Gateway | Director of Corporate Services |
| Special Category Appropriate Policy | Gateway | Data Protection Officer |

**Change Log**

| Location | Change from deletion/addition | Change to |
|---|---|---|
| | General updates/formatting throughout. | |
| Section 6 | Defined Special Category Data | |
| Section 7 | New Section - Lawful basis for processing criminal offence data. | |
| Section 8 | Individual Rights – included information on how data subjects can submit requests | |
| Section 9 | New Section - Data Protection Complaints as per Data (Use and Access) Act 2025 | |
| Section 15.3 | Reinforce that all requests from law enforcement should be referred to DPO | |

**Communication**

| | |
|---|---|
| **Who needs to know (for action)** | All Staff |
| **Who needs to be aware** | All Staff |

**Communication Plan**

| Action | By Whom | By When |
|---|---|---|
| Upload to Gateway and Website | Data Protection Officer | On approval |
| Circulation to key staff | Data Protection Officer | On approval |

**Document Development**

Details of staff who were involved in the development of this policy:

| Name | Role |
|---|---|
| Joanne Lucas | Risk & Compliance Officer |

Details of staff, external groups or external organisations who were consulted in the development of this policy:

| Name | Organisation | Date |
|---|---|---|
| FE Sector Data Protection Officers | | 19 April 2021 |

**Approval Dates**

| Approved by | Date |
|---|---|
| Governing Body | 04 November 2026 |

**Document History**

| Issue no. under review | Date of review: | Persons involved in review | Changes made after review? Yes/No If Yes refer to change log | New Issue No. | If changes made was consultation required? | If changes made was Equality Screening required? |
|---|---|---|---|---|---|---|
| V1.0 | April 2021 | J Lucas<br>Lindsey Johnston | Yes | V2.0 | No | No |
| V2.0 | March 2023 | J Lucas | No | V3.0 | No | No |
| V3.0 | May 2025 | N Nugent | Yes | V4.0 | No | No |
| V4.0 | July 2026 | N Nugent | Yes | V4.1 | No | No |