SPECIAL CATEGORY DATA APPROPRIATE POLICY DOCUMENT

Policy Owner:	Risk & Compliance Officer
Date Approved:	17/11/2021
Version:	V1.0
Equality Screening Date:	TBC
Date of First Issue:	September 2021
Date of Next Review:	June 2023
Location:	Gateway

Related Documentation

Title	Location	Owner
Data Protection Policy (UK GDPR) V2.0	Gateway SWC Website	Risk & Compliance Officer
Data Subject Rights Procedure V2.0	Gateway	Risk & Compliance Officer
FE Retention and Disposal Schedule	Gateway	Risk & Compliance Officer
Access to Information Policy V1.0	Gateway	Risk & Compliance Officer
GDPR Handbook	Gateway	Risk & Compliance Officer

Change Log

Location	Change from deletion/addition	Change to
	New Policy	

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 SWC website	J Lucas	On approval
Circulation to all staff	J Lucas	On approval

Contents

1. Introduction

When processing personal data, the College will comply with the requirements of the UK General Data Protection Regulations (UK GDPR), the Data Protection Act (2018) (DPA) and any associated legislation. The College is required to have an Appropriate Policy Document in place setting out and explaining our procedures and policies in relation to the processing of special category data.[1]

This Appropriate Policy Document for the College meets the requirement under Schedule 1, Part 4 of the Data Protection Act to:

- Explain the College's policies and procedures for ensuring compliance with the Article 5 Principles of the UK GDPR; and
- Explain our policies and procedures in regards to the retention and erasure of personal data.

The Data Protection Act (2018) outlines safeguards for the processing of sensitive special category data. Sensitive processing is defined in Article 9 of the GDPR as:

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

When processing special category data the College will ensure it has identified it's lawful basis for processing as set out in Articles 9(2) and 10 of the UK GDPR including:

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

[1] Data Protection Act 2018, Part 4, para 39

2. Relevant Schedule 1 Conditions and Data Processing Activities

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

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

- Employment, social security and social protection
    - Processing personal data concerning health in connection with the College's rights under employment law (eg processing necessary in response to the COVID-19 pandemic),
    - Processing data relating to criminal convictions in connection with the College's rights under employment law in connection with recruitment, discipline or dismissal,
    - Providing human resources and occupational health facilities for employees.

2.2 Substantial Public Interest Conditions

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

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

- Preventing or detecting unlawful acts
    - Processing necessary to ensure the safeguarding and protection of the College's students, by virtue of Paragraph 36 of Schedule 1 of the DPA Act it is not necessary to demonstrate a substantial public interest in the above processing.

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

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

- Support for individuals with a particular disability or medical condition
    - Is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,
    - Is necessary for the purposes of providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other.

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

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

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

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

2.3 Additional Conditions Relating to Criminal Convictions, etc.

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

3. Procedure for Securing Compliance

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

3.1 **Principle 1** *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*.

The College will:

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

3.2 **Principle 2** *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

The College will:

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

3.3 **Principle 3** *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

The College will:

- Only collect the minimum personal data required for the purpose for which it is collected.

- Ensure that the personal data collected is adequate and relevant.

3.4 **Principle 4** *Personal data shall be accurate and, where necessary, kept up to date.*

The College will:

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

3.5 **Principle 5** *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed*.

The College will:

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

3.6 **Principle 6** *Personal data shall be processed in a manner that ensures appropriate security of processing the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

The College will:

- Ensure that there is the appropriate organisational and technical measures in place to protect personal data.
- Ensure staff have completed mandatory training in data protection.

4. Accountability Principle

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

- Ensuring that records are kept of all personal data activities, and that these are provided to the Information Commissioner on request. The College maintains a Record of Processing Activities (Art. 30, GDPR) which records all of our personal data activities.

- Carrying out Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate

- Ensuring a Data Protection Officer is appointed to provide independent advice and monitoring of the College's personal data handling, and that this person has access to report to Senior Management

- Having in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

5. Data Retention

Personal data is held and disposed of in line with the FE Sector Retention and Disposal Schedule. When disposing of information, the College will ensure this is carried out in line with the Data in Transit Policy and destroyed securely.

6. Data Protection Officer

The DPO is the point of contact for anyone who wishes to exercise any of their data protection rights or respond to general queries. You can either write to or email on:

Data Protection Officer
SWC Cookstown Campus
Burn Road
Cookstown
BT80 8DN

(028) 8225 0109
gdpr@swc.ac.uk

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

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

Phone: 01625 545 700
Website: https://ico.org.uk

Signed Chief Executive 
Date 17.11.21

Signed Chair of the Board of Governors 
Date 17/11/2021

Document Development

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

Name	Role
Joanne Lucas	Risk & Compliance Officer & DPO

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

Name	Organisation	Date
FE Sector DPOs	All Colleges	August 2021

Approval Dates

Approved by	Date
Governing Body	17/11/2021

Document History

Issue no. under review	Date of review:	Persons involved in review	Changes made after review? Yes/No	If changes have been made, please provide brief details:	New Issue No.	If changes made was consultation required?	If changes made was Equality Screening required?
	New Policy						