TITLE	REF	VERSION
Data Protection Appropriate Policy Document	DP01	1.0

APPROVAL BODY:	DATE	REVIEW DATE
Corporation	Sep 2025	Sep 2027

LEAD PERSON	Group Head of Risk & Resilience		
EQIA DATE	N/A	DPIA DATE	N/A

DATA PROTECTION APPROPRIATE POLICY DOCUMENT

As required under Data Protection Law

Introduction

This policy has been developed by Activate Learning (hereafter referred to as the College) to meet the requirement under Data Protection law for an Appropriate Policy Document (APD). The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require that an APD is in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document will demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles

The College needs to process personal data about its current and former staff, learners, governors, and customers of its facilities to carry out its functions as a provider of further and higher education. As part of its operations, it is also necessary for the College to process special category data.

Special category data (defined by Article 9 of the UK General Data Protection Regulation (GDPR)) and sensitive data (defined by section 35 of the Data Protection Act 2018 (DPA)) is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or 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

Article 10 UK GDPR applies to the processing of personal data relating to criminal convictions and offences or related security measures.

Section 11(2) of the DPA 2018 provides that criminal offence data includes data which relates to the alleged commission of offences and related proceedings and sentencing. Information about victims and witnesses of crime is also included in the scope of data relating to criminal convictions and offences.

This policy meets the requirement in the DPA 2018 for an appropriate policy document which details the lawful basis and conditions for processing and safeguards the College has put in place when processing special category data and criminal offence data.

Description of Data Processed

The College Privacy Notice has more information about the information processed by the College, the legal basis for processing and what the information is used for.

The College processes special category personal data in the following circumstances.

As an employer. Special category data about employees are processed because it is necessary to fulfil the College's obligations as an employer. This includes information about our employees':

- health, for the following purposes:
  - to discharge our health and safety obligations
  - to determine our employees are fit to work
  - to handle staff sickness and absence records
  - to support employee wellbeing, including in order to make any necessary adjustments for disability, such as accessibility alterations to our facilities and facilitating any additional needs such as library access.

- ethnicity and sexual orientation (in relation to our equal opportunities monitoring); and
- membership of any trade union (for taking payroll deductions only)

Further information about this processing can be found in the College privacy notice.

As a place of study. Special category data about students and applicants to the College are processed. This includes information in relation to their:

- health and wellbeing (in order to provide support in relation to their health and wellbeing, including in order to make any necessary adjustments for disability, such as accessibility alterations to our facilities); and
- ethnicity and sexual orientation (in order to monitor compliance with equality legislation).

Further information about this processing can be found in the College privacy notice.

Special Category Data. The College processes special category personal data under the following legal basis:

- Article 9(2)(a) – explicit consent. An example of which would include health information we receive from learners who require additional support.
- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the College or the data subject in connection with employment, social security, or social protection. For examples where the College processes staff sickness and absences information.
- Article 9(2)(c) – where processing is necessary to protect vital interests. An example of this processing would be using health information about a member of staff or learner in a medical emergency.
- Article 9(2)(f) – for the establishment, exercise, or defence of legal claims. Examples of this processing include processing relating to any employment tribunal or other litigation.
- Article 9(2)(g) – reasons of substantial public interest. For example, to comply with other obligations imposed on the College in its capacity as a public authority e.g., the Equality Act.
- Article 9(2)(i) – where processing is necessary for public health. For example, in relation to the College's processing of data in response to the Covid-19 pandemic.

- Section 10(3) of the DPA 2018 sets out that for processing of special categories of personal data and criminal offence data to be necessary for reasons of substantial public interest under Article 9(2)(g) of the UK GDPR, that processing must meet one of the conditions set out in Part 2 of Schedule 1.

The College processes special category and criminal offence data in the performance of its statutory and corporate functions when the following conditions set out in the following paragraphs of Part 1 and Part 2 of Schedule 1 to the DPA 2018 are met:

- Part 1: Paragraph 1 (Employment, social security, and social protection)
- Part 1: Paragraph 2 (Health or social care)
- Part 1: Paragraph 3 (Public health)
- Part 1: Paragraph 4 (Research)
- Part 2: Paragraph 5 (Substantial Public Interest Conditions)
- Part 2: Paragraph 6(1) and (2)(a) (Statutory and government purposes)
- Part 2: Paragraph 8 (Equality of opportunity or treatment)
- Part 2: Paragraph 9 (Racial and ethnic diversity at senior levels of organisations)
- Part 2: Paragraph 10 (Preventing or detecting unlawful acts)
- Part 2: Paragraph 11 (Protecting the public against dishonesty etc
- Part 2: Paragraph 12 (Regulatory requirements relating to unlawful acts and dishonesty
- Part 2: Paragraph 14 (Preventing fraud)
- Part 2: Paragraph 17 (Counselling)
- Part 2: Paragraph 18 (Safeguarding of children and of individuals at risk)
- Part 2: Paragraph 20 (Insurance)
- Part 2: Paragraph 21 (Occupational pensions)
- Part 2: Paragraph 24 (Disclosure to elected representatives)

Criminal Offence Data

The College also processes criminal offence data under Article 10 of the GDPR. As an employer, the College processes criminal offence data in relation to pre-employment checks and declarations by an employee or prospective employee (in certain roles).

As a place of study, the College processes criminal offence data in relation to courses where a DBS check is required, or where the Collegey Student Membership and Disclosure and Barring Service Check Policy deems one is necessary.

Compliance with the Data Protection Principles

In accordance with the accountability principle, the College maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. The College will carry out data protection impact assessments (where appropriate) in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and default.

The College follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for processing, as follows:

- **Accountability Principle.** The College has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:
    - The appointment of a data protection officer who reports directly to the highest management level.
    - Taking a 'data protection by design and default' approach.
    - Maintaining documentation of processing activities.
    - Adopting and implementing data protection policies.
    - Implementing contracts with data processors.
    - Implementing appropriate security measures in relation to the personal data.
    - Carrying out data protection impact assessments (where required).
    - Regular review of accountability measures.
- **Principle (a): Lawfulness, Fairness, and Transparency.** The College provides clear and transparent information about the processing of personal data including the lawful basis for that processing in the College's Records of Processing Activities (ROPA) within the online GDPR Management System 'GDPR Sentry', the Privacy Statement on

the College website, within the Data Protection procedural manual, within the Data Protection and Information Security Policy and this policy document.

- **Principle (b): Purpose Limitation.** The College processes personal data for purposes of substantial public interest as explained above when the processing is necessary to fulfil statutory and corporate functions. The College is authorised by law to process personal data for these purposes. Where the College shares data with another organisation, the College shall document that sharing and implement a data sharing agreement (where required). The College shall not process personal data for purposes incompatible with the original purpose it was collected for.

- **Principle (c): Data Minimisation.** The College shall collect personal data necessary for the relevant purposes and ensure it is not excessive. The information processed is necessary for and proportionate. Where personal data is provided to the College or obtained but is not relevant to our stated purposes, it will be erased.

- **Principle (d): Accuracy.** The College shall ensure that where personal data is identified as inaccurate or out of date, having regard to the purpose for which it is being processed, and the College will take every reasonable step to ensure that data is erased or rectified without delay. If the College decides not to either erase or rectify it, for example because the lawful basis means those rights don't apply, the decision will be documented.

- **Principle (e): Storage Limitation.** All special category data processed by the College for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in Retention Procedure. This retention procedure is reviewed regularly and updated when necessary.

- **Principle (f): Integrity and Confidentiality (Security).** The College ensures that electronic information is processed within our secure networks, and the College has obtained the Cyber Essentials Plus certification. Hard copy information is processed in line with our information security and data protection procedures. The systems used to process personal data allow data to be erase or updated as required. Electronic systems and physical storage have appropriate access controls applied.

References

This Policy has been based on the ICO Appropriate Policy Document and HMRC Appropriate Policy Document and has been produced under the Open Government Licence

- ICO Appropriate Policy Document

- HRMC Appropriate Policy Document

This Policy complies with the following legislation:

- Data Protection Act 2018
- General Data Protection Regulation 2018
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003

This Policy should be read in conjunction with the following Activate Learning Policies and Procedures:

- IT Services Acceptable Use Policy
- Data Protection Handbook
- Direct Marketing Guidelines