College Data Policy

Status:	**Approved by Audit Committee Nov 2023**
Date of Version:	**November 2023**
Responsibility for Contents:	**VP Infrastructure & Communications**
Responsibility for Review:	**Corporate Governance and Planning Officer**
Review Date:	**November 2026**

1.0 Purpose

This document and associated procedures referred to in this document outlines Forth Valley College's ('the College') approach to the management of personal data, particularly special category and criminal conviction data processed by the College, as required by the UK General Data Protection Regulation (UK GDPR), Article 9 and the Data Protection Act 2018, Schedule 1, Part 4.

2.0 Policy Statement

Forth Valley College processes special category and criminal conviction data as part of its statutory duties under employment and social protection law, and for reasons of substantial public interest. The College will detail its procedures for compliance with the principles of Article 5 of the UK GDPR, and outline its policies as regards retention and erasure of this data.

3.0 Responsibility for the Implementation of this Policy and Associated Procedures

This policy applies to all College staff processing personal data, special category personal data, protected characteristics data, and criminal convictions data.

4.0 Definitions

4.1 Criminal conviction data is the data processed relating to criminal convictions and offences, or related security measures (UK GDPR, Article 10). The most common processing of this data in the College is when staff are checked for recorded criminal convictions with Disclosure Scotland under the Protecting Vulnerable Groups (PVG) scheme. Students may also be Disclosure Scotland checked, for example if their course includes a placement at a nursery or requires them to work with children or vulnerable adults.

4.2 Special category data is defined by UK GDPR Article 9(1):

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic and biometric data used to identify an individual
- Health data
- Sexual/ sex life data
- Sexual orientation

4.3 **Protected Characteristics**, as defined under the Equality Act 2010 (Article 4), should be treated as Special Category Data for data processing purposes and include:

- age;
- disability;
- gender reassignment;
- marriage and civil partnership;
- pregnancy and maternity;
- race;
- religion or belief;
- sex;
- sexual orientation.

5.0 What Laws Apply

Due to the sensitive nature of special category data, protected characteristic data and criminal convictions data, there are a number of laws in place to restrict and manage processing of this information by organisations, including Colleges. Other laws oblige the College to process such data for specific purposes. The three areas of legislation most relevant at this time are described below. Note that, should any of these legislative vehicles be superseded during the period of this policy, then the most relevant legislation will be deemed to be covered by this policy.

5.1 UK General Data Protection Legislation (UK GDPR)

GDPR is EU (European Union) legislation which came into force on 25 May 2018. UK GDPR is legislation which came into force in the UK on 31/12/20, due to the UK's exit from the European Union. UK GDPR was created by amendments in the The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

The reason for this legislation is to ensure that the privacy rights of individuals are upheld by organisations, including Colleges, that process personal data. Organisations must only process personal data where it is lawful and fair to do so; be transparent in how they process this data; process the data only for the purpose it was collected; only request the minimum amount of data required for the purpose; ensure the data is accurate, up-to-date, and not kept longer than necessary; and is processed using technical and organizational measures that ensures the security of the data.

UK GDPR provides protection to personal data; that is information that relates to a clearly identifiable living individual, for example a student or a member of staff.

UK GDPR supports an individuals' rights in relation to the personal data an organisation, such as a college, processes; including being made aware of how their data is processed; requesting copies of some or all of this information, or requesting that their information is changed, updated, or deleted; and restricting processing of their data.

Most personal data collected by the College from students and staff is processed on the basis of contract (Article 6(1)(b), or public task (Article6(1)(e)). Most special category and protected characteristics data is collected by the College on the basis of employment and social protection law (Article 9(2)(b) or substantial public interest (Article9(2)(g)). Criminal convictions data collected by the College is done so in-line with Article 10 of the GDPR, which stipulates that processing can only be carried out under the control of official authority, or when the processing meets the requirements of the Data Protection Act 2018 (see below), with appropriate safeguards in place to protect the rights and freedoms of data subjects.

5.2 Data Protection Act 2018 (DPA 2018)

The DPA 2018 enacted the EU GDPR law into UK law and establishes additional safeguards for handling special category and criminal conviction data (Schedule 1, Part 4):

- an appropriate policy document (this document);
- outlining how the controller's procedures comply with the UK GDPR Principles (Article 5) (e.g. Data Protection Policy/Procedure/Guidance);
- outlining the controller's policies on retention and deletion of data, and whether policies are strictly adhered to;
- retaining and reviewing policy document(s);
- making this document available to the Information Commissioner's Office upon request.

5.3 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

The Privacy and Electronic Communications Regulations (PECR) sit alongside the DPA 2018 and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts, and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

6.0 UK GDPR Article 5 Compliance

The College complies with the UK GDPR Principles under Article 5, as outlined in the College Data Policy, and underlying procedural documents which are available on the College intranet.

1. Lawfulness, fairness, and transparency

The College will regularly review forms and other methods of gathering data, to ensure that the processing is fair and lawful. The College will be transparent with data subjects and publish privacy notices where appropriate.

2. Purpose limitation

The College will ensure that data is only processed for the purposes listed in the Information Asset Register (Records of Processing Activity).

3. Data minimisation

The College will not collect or process data for which there is not a listed purpose in the Information Asset Register (Records of Processing Activity).

4. Accuracy

The College will ensure, wherever possible, that data subjects can access and update their records, to ensure accuracy.

5. Storage limitation

Data will be securely deleted at the end of the listed retention periods. Departmental retention schedules can be found on the College intranet.

6. Integrity and confidentiality (security)

The College will make every effort to ensure the security, integrity, and confidentiality of data. The College IT Security Policy is available on the College intranet. The College is Cyber Essentials certified.

7. Accountability

The College will keep detailed records relating to compliance and accountability issues and will record these in a version of the Information Commissioner's accountability tracker. The College has a local data protection risk register, which is constantly reviewed to address issues and risks as they arise.

7.0 Staff Training

The College will ensure all staff are trained in data protection, specifically relating to personal, special category and 'protected characteristics' data and the legislation underpinning this (see Section 5.0 above). This training will be periodically refreshed and will form part of the induction process for all new staff.

8.0 Advice for Staff

While all staff will receive training (outlined in Section 7.0 above), the College recognises that staff may either require specialist advice or assistance where a request for personal and/or College information goes beyond what a reasonable member of staff would consider a normal request for someone in their role.

Staff should, in the first instance, discuss their query with their line manager. Should your line manager be unavailable (e.g. on leave or off ill) you should contact the Data Protection Officer at dataprotection@forthvalley.ac.uk for advice as soon as possible.

9.0 Special Category Data: Lawful bases

Special category and/or 'protected characteristics' staff and student data will be processed by the College for a number of reasons related to, and compatible with, the specified purpose for which it was originally collected (as outlined in the College Privacy Notices).

9.1 Staff

The College processes various types of special category data for employees, including:

- Sickness absence data
- Occupational health data
- Health and safety data
- Disciplinary and grievance procedure data
- Trade Union membership data
- Equality and diversity data
- Protected Disclosure data

Article 6 and 9 lawful bases for all data held by the College are available on the College intranet in the Information Asset Register (Records of Processing Activities).

9.2 Students

The College processes special category data related to students, including:

- Equality and diversity data
- Counselling data
- Health and safety data
- Safeguarding data
- Personal learning support plans
- Personal escape plans

Article 6 and 9 lawful bases for all data held by the College are available on the College intranet in the Information Asset Register (Records of Processing Activities).

10.3 Exceptional circumstances

There may be exceptional circumstance where the College may have to share special category or 'protected characteristics' data using a different lawful basis, including but not limited to:

An emergency

For example, where a student or member of staff is in a critical situation, the College may have to share special category data to a paramedic, or other health worker:

- UK GDPR Article 6(1)(d) – vital interests
- UK GDPR Article 9(2)(c) – vital interests

Legal claims

For example, where the College is approached and asked to provide data on staff or students necessary to establish, exercise or defend a legal claim or as evidence for court:

- UK GDPR Article 6(1)(c) – legal obligation
- UK GDPR Article 9(2)(f) – legal claims

11.0 Criminal Convictions Data: Lawful Bases

The College has a statutory duty to protect children and vulnerable adults, as outlined in the Protection of Vulnerable Groups (Scotland) Act 2007. Where appropriate, the College will conduct criminal convictions checks to ensure that staff in contact with children and vulnerable adults do not pose a threat to their safety.

Similarly, the College will conduct criminal convictions checks to ensure that students undertaking a course where they will be in contact with children and vulnerable adults do not pose a threat to their safety.

This means that the College processes staff and/or student criminal convictions data on the following legal bases:

- UK GDPR Article 6(1)(c) – legal obligation
- UK GDPR Article 9(2)(g)- reasons of substantial public interest
  DPA 2018, Sch 1, Part 2, 18 – safeguarding of children and individuals at risk (Protection of Vulnerable Groups (Scotland) Act 2007)

12.0 Retention and Erasure

The College retains the data defined in this policy for the minimum periods of time required to meet its statutory duties. The Data Retention Schedules can be found on the College intranet.

13.0 Policy Management

This policy will be reviewed periodically and will be made available to the ICO (Information Commissioner's Office), upon request and without charge. It will be held and reviewed until a period of at least 6 months after the College has ceased processing such data.

14.0 Related Policies

Data Breach Procedure
Data Sharing Procedure
IT Security Policy
Health and Safety Policy
Safeguarding Policy
Data Subjects' Rights Procedure
DPIA Procedure
Equal Opportunities Procedure
Corporate Parenting Policy

Appendix 1 – Overview of College Data Management Procedures