There is a Welsh version of this document available.

Data Protection Policy

Scope and Purpose of Policy

This policy provides a framework for ensuring that Cardiff and Vale College (CAVC) meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It applies to all the processing of personal data carried out by CAVC including processing carried out by joint controllers, contractors, and processors.

CAVC complies with data protection legislation guided by the six data protection principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation.

The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by Victoria Davies, Director of Information and Planning (dataprotection@cavc.ac.uk). Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer.

Information covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convections and offences)

Policy Statements

This policy is underpinned by the Group's vision – Inspirational, Inclusive and Influential and will support our work towards the key drivers of Quality, Efficiency and Growth. The policy will incorporate the following principles:

- *Those who access Cardiff and Vale College Group must be* ***free from discrimination****.*
- *Learners will be supported to* ***enable*** *them to achieve their* ***potential*** *whilst in learning, in an environment which removes or minimises disadvantage, takes steps to meet their needs and which encourages participation.*
- *We will support learners to develop the skills they need to* ***progress*** *successfully through their lives.*

CAVC is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about learners, staff, customers or those who work or interact with us.

Information Asset Owners – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid CAVC in managing personal data and its associated risks.

Privacy Notices - we publish a privacy notice on our website and provide timely notices where this is required. We track and make available any changes in our privacy notice. We also publish a staff privacy notice and keep it up to date

Training - we require all staff to undertake mandatory training on information governance and security which they re-take every two years, the first is taken at induction.

Breaches - we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess on a case-by-case basis

whether we need to report breaches to the ICO and make data subjects aware of the breach.

Information Rights - we have a dedicated team and clear processes to handle subject access requests and other information rights requests.

Data Protection by Design and Default - we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

Records of Processing Activities (ROPAs) - we record our processing activities and publish our safeguards policy on law enforcement processing and processing of special category data.

Contracts - Our Commercial legal department oversee that our contracts are compliant with UK GDPR

Higher Education – the College will link to the appropriate sections of specific (data protection) policies of partner higher education providers.

Application of Policy

Staff

This policy covers not only current employees and workers but also applicants for employment, interview candidates and ex-employees.

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 CAVC from time to time. Any failure to follow the policy may result in disciplinary proceedings.

Staff are required to inform the Human Resources Team in writing of any changes to the information held as soon as possible, e.g. change of name, address, contact telephone number, bank details.

Learners

By enrolling with CAVC a student has agreed to be bound by CAVC Enrolment conditions. A student who ignores his/her responsibilities may find the student disciplinary regulations being invoked.

Students must:

- check that the information on their enrolment form is accurate.

- promptly inform CAVC in writing of any changes to the information held, i.e. change of name, address, telephone numbers, emergency contact details.

Clients

Information on CAVC clients will be of a financial or contractual nature and will be held for specified purposes e.g. payment processing.

Where information needs to be shared with external CAVC partners or clients a separate legal agreement must be signed by both parties.

Processing Sensitive Personal Data

Sometimes it is necessary to process Sensitive Personal Data. This may be to ensure that CAVC is a safe place for everyone or to operate other CAVC policies, such as the Equality and Diversity Policy and Safeguarding Policy.

CAVC will ask for information about particular health needs, such as allergies to particular forms of medication, or other conditions such as asthma or diabetes. CAVC will only use this information to protect the health and safety of the individual.

It is appreciated that processing sensitive personal data may cause concern. CAVC's policy, where possible and appropriate, is to seek consent from data subjects before collecting or otherwise processing sensitive personal data. It will not, however, always be appropriate to seek consent or necessary to do so. For example, in certain circumstances CAVC may be processing sensitive personal data fairly and lawfully if at least one of the following conditions is satisfied:

- The processing of the information is necessary for the performance of CAVC's obligations under employment law;
- The processing is necessary for the purpose of obtaining legal advice, the administration of justice or exercising public functions;
- The processing is necessary in order to protect the vital interests of the data subject or another person;
- The data is processed in relation to equal opportunity monitoring.

Subject Access Request

Under the Act, staff, students and other users of CAVC have the right to:

- Be told whether their personal data is being processed;
- Be given a description of the data concerned;
- Be informed about the purposes for which it is being processed;

- Be informed of the identity of third parties to whom data may be disclosed;
- Request a legible copy of their personal data.

Individuals seeking to access personal data under the Act must provide to the Data Protection Officer the following:

- a request in writing, (either electronic or hard copy; the request need not make reference to the Act);
- sufficient information to enable CAVC to:

- verify the identity of the individual (such as a utilities bill or staff or student identification card and a certified copy of another piece of identity); and
- identify what information the individual requires, and where that information might be held.

CAVC may ask for further information if required to locate the data requested.

CAVC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one calendar month.

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer to provide than other information. For further information, refer to CAVC's Freedom of Information Policy and related procedures.

There are a number of exemptions under the Act to the right to access personal data. Where CAVC is unable to comply with a subject access request in full or in part, it will set out the reasons why it is unable to do so.

Data Storage and Retention

Information will be stored in a manner which provides for reasonable access in terms of the purpose for which the information is held. Appropriate technical and organisational measures shall be taken for preventing unlawful processing of data and accidental loss or destruction of personal data. To ensure this, CAVC has separate Data Retention guidelines covering:

- The physical storage of records i.e. staff guidelines on best practice storage methods, retention periods and destruction periods.
- Networked data storage i.e. staff/student IT acceptable use procedures, network security, server backup and off-site access.

Use of Artificial Intelligence (AI) and Automated Processing with Data

CAVC recognises the increasing role of AI in data processing and decision-making. To ensure that AI technologies are used in a way that is compliant with the UK GDPR and DPA 18, the following principles will be adhered to:

- Lawful Basis for Processing: The use of AI for processing personal data will be based on a lawful basis (e.g. consent, performance of a contract, legitimate interests), in line with GDPR requirements.

- Data Minimisation: AI systems will only process the personal data that is necessary for the specified, legitimate purposes, and ensure no excessive data is used.
- Bias and Fairness: CAVC is committed to ensuring that AI systems are free from discrimination and bias.
- Data Protection Impact Assessments (DPIAs): Where AI involves high-risk processing, DPIAs will be conducted to assess the impact on individuals' rights and freedoms, ensuring proper safeguards are in place.*
- Human Oversight: Significant decisions impacting individuals, such as automated decisions related to admissions or grading, will involve human review to ensure fairness and transparency.
- Staff Training: CAVC staff receive periodic training on how to use AI tools in compliance with data protection regulations. This includes the importance of not using personal data in training large language models (LLMs) or other AI systems without explicit informed consent from the individuals whose data is involved.
- Right to Object: Individuals will have the right to object to automated decision-making or profiling where applicable under the GDPR, and alternative arrangements will be made to review such decisions manually.

*A Data Protection Impact Assessment (DPIA) is a process required under the UK GDPR for organisations to identify and minimise the data protection risks of a project, particularly when introducing new technology, such as Artificial Intelligence (AI).

What this means in the context of AI:

- High-risk processing refers to any processing of personal data that could pose significant risks to individuals' rights and freedoms. In AI, this might include:
    - Automated decision-making (e.g., AI deciding admissions or grading).
    - Profiling individuals based on their data (e.g., predicting student performance).
    - Using sensitive or special category data (e.g., health or biometric data).
- A DPIA assesses these risks by:
    - Identifying the personal data involved, the processing activities, and the purpose of the AI system.
    - Evaluating how the AI might affect individuals, such as whether it could lead to discrimination, unfair outcomes, or violations of privacy.

    - Mitigating risks by implementing safeguards (e.g., limiting the data used, adding human oversight to automated decisions, anonymising data).
- The purpose of the DPIA is to ensure that appropriate safeguards are in place, such as:
    - Data minimisation (using only the necessary data).
    - Strong encryption or pseudonymisation.
    - Procedures to ensure individuals' rights are respected (e.g., the right to object to automated decisions).

In short, the DPIA helps ensure that when AI is used in high-risk scenarios, the impacts on individuals' privacy, data protection, and rights are carefully considered and properly managed before deploying the technology.

Misuse of Data

Any member of staff/student who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Officer initially. If the matter is not resolved it may be raised as a formal complaint by following the complaints procedure
This policy applies to:

- All learners within CAVC, regardless of mode or location of study.
- All staff within CAVC.
- All partners and franchise organisations.
- Visitors to CAVC.

Responsibilities

The Governing Body is responsible for ensuring that:

- The Policy is reviewed on a regular basis (as per the policy terms of review) and appropriate advice is given on content. The Main Board approves the policy.
- They act in accordance with the policy and associated procedures.

The Executive and Senior Leadership Team are responsible for:

- Developing effective governance arrangements and ensuring that relevant policies are in place across CAVC.
- Reviewing this Policy and the attached procedures.
- Ensuring sufficient resources are in place to carry out the duties outlined.
- Ensuring staff have sufficient training.

The Director of Information and Planning is responsible for:

- Maintaining the currency of this policy and associated procedures.
- Ensuring appropriate steps are taken to monitor data linked to this policy and that this data is used to inform and improve practice.

The Senior Quality Staff are responsible for:

- Providing appropriate training and development and support for staff to ensure they can follow the policy.

All Teaching and Skills Support Staff are responsible for:

- Acting in accordance with the policy and associated procedures and inform their line managers of any activity contrary to the principles outlined.
- Attending relevant CPD events.

Learners are responsible for:

- Acting in accordance with the policy and associated procedures and informing their tutor of any activity contrary to the principles outlined.
- Attending induction sessions related to this.

Equality and Diversity Statement

In accordance with College procedures, this Policy was written with consideration of the impact of individuals as per the Equality Act.

Welsh Language Standards

This policy provides opportunities for persons to use either the Welsh or English language. The duties which come from the Standards mean that organisations should not treat the Welsh language less favourably than the English language, together with promoting and facilitating the use of the Welsh language i.e. making it easier for people to use in their day-to-day life.

Health and Safety Implications

There are no Health and Safety implications for this policy. Any H&S implications of research activities will be covered by the research procedures.

Linked Policies

- Equality and Diversity
- Safeguarding

Linked Procedures

- Data Protection Procedure
- CAVC Privacy Notice
- Staff Privacy Notice
- Equality and Diversity
- Safeguarding
- Data Retention
- Freedom of Information
- Dress code

Approval, Change and Review

This policy is reviewed every two years.

Location and Access to the Policy

This policy is available from the college website. A copy of this policy is available in Welsh.

Date approved:	October 2024	**Responsible Manager**:	Director of Information & Planning
Approved by:	Main Board	**Executive Lead:**	Group Chief Operating Officer
Review date:	October 2026	**Accessible to Students:**	Yes