Data Protection Policy

Scope and Purpose of Policy

Everyone has rights with regard to how their personal information is handled. Cardiff and Vale College (the "**College**" or "**we**" or "**us**") holds a variety of information on individuals, stored both manually and electronically, which is governed by the principles of the Data Protection Act 2018 (the "**Act**").

The information which the College holds, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified Act and other regulations. The Act imposes restrictions on how the College may use that information.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

Status of the policy

This policy has been approved by the College's Governing Body. It sets out the College's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by Evan Davies, Director of Information Services and Technology, 029 2025 0440, edavies@cavc.ac.uk, FOI@cavc.ac.uk and 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.

Definition of data protection terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual

(such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in connection with the College's activities.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Policy Statements

The College respects the privacy of the personal data of all its employees, students and clients and any other relevant data subjects and intends to conform to the data protection principles.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate and kept up to date.
- Not kept longer than necessary for the purpose.
- Processed in accordance with data subjects' rights.
- Kept safe and secure from unauthorised access, accidental loss or destruction.
- Not transferred to people or organisations situated in countries without adequate protection.

Fair and lawful processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject

must be told who the data controller is (in this case the College), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for limited purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

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 the College 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.

Students

By enrolling with the College a student has agreed to be bound by the College regulations. 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 the College in writing of any changes to the information held, i.e. change of name, address, telephone numbers, emergency contact details.

Clients

Information on College 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 College 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 the College is a safe place for everyone or to operate other College policies, such as the Equality and Diversity Policy and Safeguarding Policy.

The College will ask for information about particular health needs, such as allergies to particular forms of medication, or other conditions such as asthma or diabetes. The College 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. The College'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 the College 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 the College'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 the College 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 the College 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.

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

The College 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 the College'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 the College 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, the College 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.

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.

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.

Health and Safety Implications

Welsh Language Standards

This policy does not affect the Welsh language negatively. In accordance with College procedures, this Policy was written with consideration of the impact of individuals as per the Welsh Language Standards.

Linked Policies

Freedom of Information
Equality and Diversity
Disclosure
Safeguarding

Linked Procedures

Data Retention
Freedom of Information
Equality and Diversity
Disclosure
Safeguarding
Dresscode
CAVC Privacy Notice
Staff Privacy Notice

Location and Access to the Policy

This is available from the website, staff intranet and Moodle and may be out of date if printed. There is a Welsh version of this document available.

Date approved:	**17 May 2013**	**Responsible Manager:**	**Director of IS and IT**
Approved by:	**Quality Standards Board**	**Executive Lead:** :	**Chief Operating Officer**
Review date:	**14/9/2018**	**Accessible to Students:** :	**Yes**