# DATA PROTECTION POLICY

| | |
|---|---|
| **Review Schedule:** | **2 years** |
| **Originated:** | **3rd July 2014** |
| **Reviewed:** | **Autumn 2021** |
| **Next review Date:** | **Summer 2022** |
| **Responsibility:** | **Finance and Resources Committee** |

# DATA PROTECTION POLICY

## 1. General Statement

The Governing Body of Clyst Vale Community College ("the College") has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Principal and Governors of this College intend to comply fully with the requirements and principles of the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA)2018. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

## 2. Enquiries

Information about the College's Data Protection Policy is available from The College Manager and the College's Data Protection Officer. General information about the GDPR and DPA can be obtained from the Information Commissioner's Office (Information Line 0303 123 113, website www.ico.org.uk).

## 3. Fair Obtaining and Processing

The College undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

**"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

**"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.

**"personal data"** - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The College may process a wide range of personal data of staff (including governors and volunteers) students, their parents or guardians as part of its operation.

This personal data may include (but is not limited to):

- names and addresses (including email addresses),
- bank details,
- academic data e.g. class lists, pupil / student progress records, reports, disciplinary actions, admissions and attendance records
- references,

- employment history,
- taxation and national insurance records,
- appraisal records,
- examination scripts and marks

**"special category personal data" -** Personal data which is more sensitive and so needs more protection, including information about a living individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Criminal records are treated in much the same way as other special category data

**"parent"** has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

## 4. Registered Purposes

The Data Protection Registration entries for the College are available for inspection, by appointment, at the College. Explanation of any codes and categories entered is available from the College Manager who is the person nominated to deal with Data protection issues in the College. Registered purposes covering the data held at the College are listed on the College's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

## 5. Processing Personal Data

In order to ensure that the College's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- The data needs to be processed so that the College can fulfil a **contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract;
- The data needs to be processed so that the college can comply with a **legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;
- The data needs to be processed so that the College, as a public authority, can **perform a task in the public interest, and carry out its official functions** ;
- The data needs to be processed for the **legitimate interests** of the College or a third party where necessary, balancing the rights of freedoms of the individual).

However, where the College can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** The College will seek consent to process data from the pupil or parent depending on their age and capacity to understand what is being asked for.

## 6. Sharing Personal Data

Please refer to the College's Privacy Notices.

- The College will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:
  - The College will share data if there is an issue with a pupil or parent/carer that puts the safety of staff at risk;
  - The College will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or child;
  - The College's suppliers and contractors need data to provide services – for example, IT companies. When sharing data the College will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares where there is regular sharing ;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the College.
- The College may also share personal data with law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:
  - For the prevention or detection of crime and/or fraud;
  - For the apprehension or prosecution of offenders;
  - For the assessment or collection of tax owed to HMRC;
  - In connection with legal proceedings;
  - For research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.
- The College may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

## 7. Data Protection by Design and Default

The College has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.
It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment.

## 8. Data Protection Principles

The GDPR is based on 7 key data protection principles that the College complies with. The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the College will explain to individuals why the College needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The College reviews its documentation and the basis for processing data on a regular basis.

- **Collected for specified, explicit and legitimate purposes** – the College explains these reasons to the individuals concerned when it first collects their data. If the College wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ The College will document the basis for processing. For special categories of personal data, it will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** the College must only process the minimum amount of personal data that is necessary in order to undertake its work.

- **Accurate and, where necessary, kept up to date** – the College will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

- **Kept for no longer than is necessary for the purposes for which it is processed** – when the College no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule.

- **Processed in a way that ensures it is appropriately secure** – the College implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy for further information which incorporates principles around Bringing Your own Device (BYOD), the College's remote access policy, and how data is securely transferred in and out of the College's system.

- **Accountability –** The College complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:
    - Completing Data Protection Impact Assessments (DPIAs) where the College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the College will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
    - Integrating data protection into internal documents including this policy, any related policies and Privacy Notices;
    - Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the College also maintains a record of attendance;
    - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and college policies;
    - Maintaining records of its processing activities for all personal data that it holds.

## 9. Data Integrity

The College undertakes to ensure data integrity by the following methods:

### *Data Accuracy*

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the College of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the College will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

### *Data Adequacy and Relevance*

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the College will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. A printout of their data record will be

provided to data subjects every twelve months so they can check its accuracy and make any amendments.

***Destruction of records***

We apply our retention policy, and will permanently destroy both paper and electronic records securely in accordance with these timeframes.
We will securely destroy hard copies and will ensure that any third party who is employed to perform this function will have the necessary accreditations and safeguards.

If we delete electronic records and our intention is to put them beyond use, although it may be technically possible to retrieve them, we follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.
.

## 10. Subject Access Requests and Other Rights of Individuals

In all aspects of its work, the College will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the College's work. Subject to exceptions, the rights of the data subject as defined in law are;

*a) The Right to be informed.*

The College advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation such as consent forms where appropriate.

*b) The Right of access*

An individual when making a subject access request (SAR) is entitled to the following;

i. confirmation that their data is being processed;
ii. access to their personal data;
iii. other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

The College must respond to such a request within 30 days unless the request is complex, in which case it may be extended by a further 60 days. Please refer to Appendix 1 for further details as to how to manage a subject access request.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 College days in accordance with the current Education (Pupil Information) Regulations.

*c) The Right to rectification*

Individuals have the right to ask to rectify information that they think is inaccurate or incomplete. The College has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified.

*d) The Right to erasure*

The right for an individual to request that their data is erased is not absolute. It applies where:

- the information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- the information is no longer required by the College;
- a legal obligation to erase the data applies;
- the data was collected from a child for an online service;
- the College has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the College to continue to process it.

*e) The Right to restrict processing*

An individual may ask the College to temporarily limit the use of their data when it is considering:

- a challenge made to the accuracy of their data, or
- an objection to the use of their data.

In addition, the College may be asked to limit the use of data rather than delete it , if the individual does not want the College to delete the data but does not wish to it continue to use it, in the event that the data was processed without a lawful basis or to create, exercise or defend legal claims.- .

*f) The Right to data portability*

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The College only has to provide the information where electronically feasible.

*g) The Right to object*

Individuals have a right to object in relation to the processing of data for

- a task carried out in the public interest
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.
-

*h) The right to withdraw consent to processing*

*i) Rights related to automated decision making*

This does not apply as the College does not employ automated decision making processes.

## 11. Training

To meet our obligations under Data Protection legislation, we ensure that all staff, volunteers, and governors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it, for example relating to use of systems or as appropriate.

Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the College's processes make it necessary

## 12. Roles and Responsibilities

This policy applies to all staff (including volunteers and governors) who work at the College, and to external organisations or individuals working on its behalf.
**Governing Body -** The Governing Body has overall responsibility for ensuring that the College complies with all relevant data protection obligations.

**Principal -** The Principal acts with the delegated authority of the Governing Body on a day to day basis and will liaise with the DPO. In the Principal's absence, in case of emergency, this role will be delegated to the College Manager.

**All staff -** All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff; The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting data in line with this policy and the retention schedule
- Informing the College of any changes to their personal data, such as a change of address
- Reporting to the Principal, or in their absence the DPO in the following circumstances:

- Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
- If they have any concerns that this policy is not being followed;
- If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
- If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
- The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and *Personal data breaches or near misses* section of this policy.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to likely to be required please see - *Sharing Personal Data*.

## 13. Data and Computer Security

The College undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

### *Physical Security*

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the College are required to sign in and out, to wear identification badges whilst in the College and are, where appropriate, accompanied.

### *Logical Security*

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly.

### *Procedural Security*

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall Information Security Policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.
Any queries or concerns about security of data in the College should in the first instance be referred the IT Manager.

## 14. Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Principal and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of deliberate inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

## 15. Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the governing body and, where relevant, provide the College with advice and recommendations on data protection issues.

The College has appointed i-West as its DPO and they can be contacted by email at
Email: i-west@bathnes.gov.uk.
Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath

BA1 5AW

Under usual circumstances the Principal or a member of SLT will be the point of contact with the DPO.

## 16. Biometric Recognition Systems

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form the form of fingerprint, voice or facial recognition. We use biometric in the following ways.

Cashless catering payment
Follow me printing/photocopying

We will undertake a data protection impact assessment before implementing any new system to assess the impact on individuals

In accordance with the Protection of Freedoms Act 2012, once satisfied, we will notify all those will parental responsibility in the case of any student under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written parental objection. We will not proceed to process the information if the student themselves objects. Either parents or the student may withdraw their consent at any time, although parents must object in writing.

Further details on any aspect of this policy and its implementation can be obtained from:

The College Manager
Clyst Vale Community College
Station Road
Broadclyst
Exeter
EX5 3AJ

## Appendix 1 – Subject Access Request Procedure (SAR)

The school shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west), using the School SAR Guidance provided to the school.

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the school.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (i-west), and their School SAR Guidance.

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.