CHEPSTOW SCHOOL
INSPIRING LEARNING
YSBRYDOLI DYSGU

CHEPSTOW SCHOOL DATA PROTECTION POLICY

Approved by: Full Governing Body

Last Reviewed on: 03.12.2025

Next Review Date: Annual

DATA PROTECTION POLICY

School Name: CHEPSTOW SCHOOL

Date of Approval: 03/12/25
Review Date: Annual

1. Context and Purpose

- **Introduction:** Chepstow School is committed to full compliance with the Data Protection Act 1998 ["the Act"] and recognises in full the rights and obligations established by the Act in relation to the management and processing of personal data aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
- **Purpose:** This policy meets the requirements of the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act (DPA) 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Student Information (Wales) Regulations 2017, which gives parents/ carers the right of access to their child's educational record.

2. Aims and Objectives

- Ensure compliance with General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.
- Protect personal data from unauthorised access, loss, or misuse.
- Provide clear guidance on data handling and breach management.

3. Roles and Responsibilities

This policy applies to all staff employed by our school, and to parents/ carers, governors, external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action following the school's procedures.

- **School Leadership:** The Headteacher acts as the representative of the data controller on a day-to-day basis.
- **Governing Body:** The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
- **Data Protection Officer:** The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

  Our DPO is Sharon Giddy and is contactable by email at Sharongiddy@chepstowschool.net

  The Local Authority DPO is Kathryn Evans and is contactable on DataProtection@monmouthshire.gov.uk

- **Staff Members:** Staff are responsible for:
  - Collecting, storing and processing any personal data in accordance with this policy.
  - Informing the school of any changes to their personal data, such as a change of address
  - Contacting the DPO in the following circumstances:
    i. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    ii. If they have any concerns that this policy is not being followed.

iii. If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
iv. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
v. If there has been a data breach.
vi. Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
vii. If they need help with any contracts or sharing personal data with third parties.

- **Students:** Students must not share personal information about themselves or others without consent (e.g. addresses, phone numbers, photos). When using school devices, email, or online platforms, students should follow the ICT Acceptable Use Policy and avoid actions that compromise data security. If students become aware of a data breach, misuse of personal data, or suspicious activity, they should report it immediately to a teacher or the Data Protection Officer.

- **Parents/ Carers:** Will ensure all personal data shared with the school (e.g. contact details, medical information) is accurate and kept up to date. Parents/carers must not share personal information about other students, parents/ carers, or staff without consent. They should follow consent procedures by completing consent forms for photographs, videos, biometric systems, and online services promptly and honestly. They should notify the school immediately if they suspect a data breach or misuse of personal information.

4. Policy Statements

The school will comply fully with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR).

The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

5. Implementation and Procedures

Collecting Personal Data

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school 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 school, 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 school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent / carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal

data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies - we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    i Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    ii Establish a data sharing agreement 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 we share.
    iii Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.
- We are legally required to do so, with law enforcement and government bodies, including for:
    i The prevention or detection of crime and / or fraud.
    ii The apprehension or prosecution of offenders.
    iii The assessment or collection of tax owed to HMRC.
    iv In connection with legal proceedings.
    v Where the disclosure is required to satisfy our safeguarding obligations.
    vi Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.
- Emergency services and local authorities require personal data, to help them to respond to an emergency situation that affects any of our students or staff.

When we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject Access Requests and Other Rights of Individuals

Chepstow School recognises the right of all Data Subjects to access information held about them by Chepstow School and has an established procedure for responding to requests for access to such information. Chepstow School aims to comply with requests for access to personal information as quickly as possible and ensures that information is provided within the statutory 40-day limit unless there is good reason for delay.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.

Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, by letter via email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the schools DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given consent. Children aged 13 and above are generally regarded to be mature enough

to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 28 days upon receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 28 days, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time.

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental Requests to see Educational Records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request to the DPO.

Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents / carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer as well as the child before we take any biometric data from them and first process it.

Parents / carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

Parents / carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s) / carer(s).

The cashless system operated by the Cunninghams by using an image of a finger to associate it with a mathematical algorithm. The image of the fingerprint is not retained and cannot be used for any identification purposes. We take a scan of the finger and turn this image into a digital signature. The information stored cannot be used to recreate an image of the fingerprint.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the School Business Manager.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents / carers, or students for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages such as Facebook and X (Twitter)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Use of Photographs and Video by Parents, Carers and Visitors

To protect the privacy and safety of pupils and staff, parents, carers and members of the public must not take photographs or record video on the school site without prior permission from the school. This includes during events, performances, sports fixtures and any other school-based activity. Permission will only be granted where the school is satisfied that images will be used appropriately and in line with safeguarding and data protection expectations.

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- 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; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - i For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data.

ii For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff will take necessary precautions to make sure that this is kept secure following the school's ICT Acceptable use Policy.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The school will make all reasonable endeavours to ensure no personal data breaches occur. In the unlikely event of a suspected breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 24 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students and their results.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about students.

Training and Data Protection Awareness

All staff and governors with computer access are required to undertake the mandatory online training online. The Headteacher / Line Manager is responsible for ensuring the staff that fall outside this category are aware of their obligations when handling personal/sensitive information

Monitoring Arrangements

The schools DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated, if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full governing board.

6. Review and Amendments

- This policy will be reviewed annually by the Data Protection Officer (DPO) in consultation with the Headteacher and Governing Body.
- Additional reviews will take place immediately following any significant changes in legislation, regulatory guidance, or school practices that impact data protection.

Process for Modifications:

- Proposed amendments must be documented and submitted to the Governing Body for approval.
- Updates will be shared with staff, parents/ carers, and relevant stakeholders via official channels where it is deemed relevant and necessary.

7. Supporting Documents and References

This data protection policy is linked to our:

- ICT Acceptable Use Policy for Staff.
- ICT Acceptable Use Policy for Students.
- Complaints Policy – in place a complaints procedure to ensure individuals concerned about any aspect of the management of personal data are able to raise their concerns in a fair and equal way. This procedure is available from the Headteacher upon request

Appendix 1: Definitions

- **Personal data** – Any information relating to an identified, or identifiable individual. This may include the individual's:
    i Name (including initials)
    ii Identification number
    iii Location data
    iv Online identifier, such as a username

  It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

  Special categories of personal data – Personal data, which is more sensitive and so needs more protection, including information about an individual's:
    i Racial or ethnic origin
    ii Political opinions
    iii Religious or philosophical beliefs
    iv Trade union membership
    v Genetics
    vi Biometrics (such as fingerprints, retina and iris patterns), used for identification purposes
    vii Health – physical or mental
    viii Sex life or sexual orientation
- **Processing** – Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
- **Data subject** – The identified or identifiable individual whose personal data is held or processed.

- **Data controller** – A person or organisation that determines the purposes and the means of processing of personal data.
- **Data processor** – A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
- **Personal data breach** – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- **The Data Controller:** Our school processes personal data relating to parents/ carers, students, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify their line manager who will then inform the DPO by email.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost / stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been made available to unauthorised people

The DPO will alert the headteacher and the chair of governors, and make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure). The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination

- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO may contact the ICO for advice.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the 'Secure Area' of the school's network.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 24 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - i The categories and approximate number of individuals concerned.
  - ii The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 24 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- the name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts, cause and effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the 'Secure Share' areas of the schools' network. The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive Information Being Disclosed via Email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask attempt to recall the email by contacting the Schools IT Department.

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher / website owner or administrator to request that the information is removed from their website and deleted.

Other disclosures may include:

- Non-anonymised student exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked, and parents/ carers' financial details stolen.

Policy Review

Annually to ensure Chepstow School meets effectively its operational and legal requirements.