

Clytha Information Security Policy



'To Lift Ourselves and Others into our Best Future' 'I godi'n hunain a phawb ar gyfer dyfodol disglair'

Policy Written	February, 2019
Review Date	September, 2023
Next Review Date	September, 2025

Contents

1. Aims	2
2. Legislation and Guidance	2
3. Definitions	3
4. The Data Controller	4
5. Roles and Responsibilities	4
6. Data Protection Principles	5
7. Collecting Personal Data	5
8. Sharing Personal Data	6
9. Subject Access Requests (and other rights of individuals)	6
10. Parental Requests to See Educational Record	8
11. Biometric Recognition Systems	8
12. CCTV	8
13. Photographs and Videos	8
14. Data Protection by Design and Default	9
15. Data Security and Storage of Records	9
16. Disposal of Records	10
17. Personal Data Breaches	10
18. Training	10
19. Monitoring Arrangements	10
20. Links with Other Policies	13
Appendices	15

Appendix 1: Personal Data Breach Procedure

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents/legal guardians, 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](#). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the 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](#).

Whilst our school does not currently use biometric data, this policy meets the requirements of the [Protection of Freedoms Act 2012](#) should we decide to in the future.

Our school does not use CCTV cameras however this policy does reflect the ICO's [code of practice](#) for the use of surveillance cameras and personal information, should we decide to install equipment on site.

In addition, this policy complies with regulation 5 of the Education (Student Information) (Wales) Regulations 2017, which gives parents/legal guardians the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• 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 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.

4. The Data Controller

Our school processes personal data relating to parents/legal guardians, pupils, 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 as legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed by the Governing Body, Volunteers and to external organisations or individuals working on behalf of the Governing Body. Employees who do not comply with this policy may face disciplinary action following the Governing Body procedures.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring 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 Body and, where relevant, report to them 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.

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 Employees

Employees 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:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
 - 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
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that the school must comply with. The principles say 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.

7. Collecting Personal Data

7.1 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:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

- Necessary for the purpose of legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interest, rights or freedoms of the data subject.

For special categories of personal data (such as race, ethnic origin, trade union membership and health), the school will also meet one of the special category conditions for processing as set out in Article 9 of the GDPR and Data Protection Act 2018 (for further details please see www.ico.org.uk).

When offering online services to pupils, such as classroom applications, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil 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.

7.2 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.

Employees must only process personal data where it is necessary in order to do their jobs.

When Employees no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Local Authority Retention Schedule.

8. Sharing Personal Data

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

- There is an issue with a pupil or parent/legal guardian 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 pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - 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
 - 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 will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders

- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

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

9. Subject Access Requests (SAR) and other rights of individuals

9.1 Subject Access Requests

Individuals have a right to make a Subject Access Request (SAR) 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

A SAR must be submitted in writing, either by letter or by email to the DPO. They should include:

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

If an employee receives a SAR they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests (SAR)

Personal data about a child belongs to that child, and not the child's parents/legal guardian. For a parent/legal guardian 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 SAR, or have given their 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. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests (SAR)

When responding to requests, we:

- Will ask the individual to provide 2 forms of identification
- Will 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 pupil 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

We will refuse a request if:

- It is unfounded or excessive (we will charge a reasonable fee, which takes into account administrative costs)
- 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.

9.4 Other data protection rights of the individual

In addition to the right to make a SAR (see above), and to receive information when we are collecting their data about how we use and process it, (see section 7), 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). Generally, there are no decisions made in our school that solely rely upon automated decision making or profiling alone.
- 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 employees receive such a request, they must immediately forward it to the DPO.

10. 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 pupil) within 15 school days of receipt of a written request to the DPO.

11. Biometric Recognition Systems

Biometric data used as part of an automated biometric recognition system, should comply with the requirements of the Protection of Freedoms Act 2012.

Whilst we currently do not use biometric data, parents/legal guardians 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/legal guardian before we take any biometric data from their child and first process it.

Parents/legal guardian and pupils 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 pupils.

Parents/legal guardians and pupils 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.

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.

12. CCTV

We do not currently use CCTV but should we decide to in future we will inform you. 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.

13. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain consent from staff/visitors and parents/legal guardians of pupils, for photographs and videos to be taken of them for communication, marketing and promotional materials. For pupils, this is obtained during the admissions stage into the school.

Uses may (this is neither an inclusive nor exclusive list) include:

- Within school on notice boards and in school brochures, newsletters, and so on
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website, SeeSaw or School Twitter account.

Consent can be refused or withdrawn at any time, which should be done in writing. 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.

14. 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 (see section 6)
- 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:

- o 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 (via our privacy notices)
- o 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

15. 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 against 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 will not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where PCs and laptops need to be left during the working day, these should be screen locked when the workstation is left.
- Where personal information needs to be taken off site, staff will take necessary precautions to make sure that this is kept secure by following the school's ICT Policy
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices, with employees and pupils 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
- Employees, pupils or governors should generally not store personal information on their personal devices, but where this is unavoidable, are expected to follow the same security procedures as for school-owned equipment (see our ICT Policy).
- 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 (see section 8).

16. 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.

17. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 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 pupils and their results
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

These breaches may occur as a consequence of (not an inclusive nor exclusive list):

- Data being shared to incorrect recipients via email
- Hard copy data lost, missing or stolen
- Electronic devices lost, missing or stolen
- Electronic systems being compromised as a result of cyber-crime

18. Training

All Employees, Volunteers and Governors are provided with data protection training as part of their induction process by the Headteacher, Deputy Head teachers or DPO. Data protection will also form part of Continuing Professional Development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring Arrangements

The Head teacher and 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 2 years** and agreed by the Governing Body.

20. Links to Other Policies

This policy is linked to a number of school and Newport City Council policies. A copy of any such policy can be requested via the School Office.

Appendix 1: Personal Data Breach Procedure

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

1. 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 Headteacher and DPO by email.
2. 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:
 - a. Lost
 - b. Stolen
 - c. Destroyed
 - d. Altered
 - e. Disclosed or made available where it should not have been
 - f. Made available to unauthorised people
3. The DPO will alert the Headteacher and the Chair of Governors
4. The DPO will 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.
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. 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:
 - a. Loss of control over their data
 - b. Discrimination
 - c. Identify theft or fraud
 - d. Financial loss
 - e. Unauthorised reversal of pseudonymisation (for example, key-coding)
 - f. Damage to reputation
 - g. Loss of confidentiality
 - h. Any other significant economic or social disadvantage to the individual(s) concernedIf 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.
7. 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.
8. 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:
 - i. A description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned

and the categories and approximate number of personal data records concerned

- b. The name and contact details of the DPO
 - c. A description of the likely consequences of the personal data breach
 - d. 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
9. 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
10. 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:
- a. The name and contact details of the DPO
 - b. A description of the likely consequences of the personal data breach
 - c. 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
11. 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
12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- a. Facts and cause
 - b. Effects
 - c. 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 Area' areas of the school's network.
13. 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.