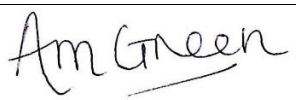
YSGOL CEFN MAWR

SCHOOL DATA PROTECTION POLICY

Learning Enjoying Achieving

September 2024

Date policy becomes effective	September 2024
Author of document	WCBC Schools DPO
Review date	November 2027
Headteacher signature	

This policy was approved by the Finance and Staffing Committee on behalf of the Governing Body on the 26th November 2024**.**

Signed on behalf of the Governing Body: 

DATA PROTECTION POLICY

1. Introduction

<< school name>> is required to ensure that appropriate controls are implemented and maintained in relation to the processing of personal data relating to its pupils, parents, staff, visitors and contractors. These controls should be enacted in compliance with the requirements of the latest UK data protection legislation.

This policy document sets out the school's intentions to fulfil its obligations under the legislation, and the arrangements it has in place to comply with it.

2. Legislation and guidance

UK General Data Protection Regulation (UK GDPR)

Data Protection Act 2018 (DPA2018)

3. Aims and purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

4. Definitions

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data controllers: are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed.

Data Privacy Impact Assessment (DPIA): a tool / assessment used to identify and reduce risks of a data processing activity.

Data Processors: include any person or organisation that is not a data user who processes personal data on our behalf and on our instructions.

Data Protection Officer (DPO): is responsible for monitoring our compliance with data protection law.

Data Subject: means a living, identified or identifiable individual about whom we hold Personal Data.

Personal Data: any information relating to an identified or identifiable natural person (data subject). Examples are a name, an identification number, location data, or an online identifier such as a username.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it.

Processing: is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Category Personal Data: includes information about a person's racial or ethnic origin, political opinions; religious or philosophical beliefs; Trade Union membership; physical or mental health or condition; genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life.

5. School as Data controller

The school acts as a Data Controller, as we process personal data relating to parents/carers, staff, governors, contractors and school visitors.

The school is registered with the ICO and pays a data protection fee to the ICO on an annual basis, as legally required.

6. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf.

- **Governing body**

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations

- **Headteacher**

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

- **School Data Protection Lead**

The school will have an assigned staff member who will be responsible for handling data protection queries.

- **School staff**

The school is committed to ensuring that all staff comply with the Act. All staff are responsible for collecting, storing and processing any personal data in accordance with this policy.

- **Data Protection Officer**

We have an assigned Data Protection Officer, who provides advice on Data Protection-related issues when required. The DPO can be contacted via the local authority at SchoolsDPO@wrexham.gov.uk

7. Data Protection principles

We will collect and use personal information in accordance with the principles of the Act, which require that:

(a) Personal data shall be processed fairly, lawfully and with transparency
(b) Personal data shall be obtained only for specified and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. ('Purpose limitation')
(c) Personal data held for any purpose should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. ('Data minimisation')
(d) Personal data shall be accurate and, where relevant, kept updated. Every reasonable step will be made to ensure that inaccurate personal data is erased or rectified without delay. ('Accuracy')
(e) Personal data should be kept in a form that permits the data subject to be identified for no longer than is necessary for processing. ('storage limitation')
(f) Personal data must be processed in a manner that ensures its security ('integrity and confidentiality')

8. Lawfulness, fairness and transparency

We will only process personal data when we have a lawful basis to do so. There are six lawful bases for processing data set out under Article 6 of UK GDPR legislation, and at least one of these must apply for us to process personal data.

(a) **Consent:** the data subject has given clear consent for us to process their personal data for a specific purpose.
(b) **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
(c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
(d) **Vital interests:** the processing is necessary to protect someone's life.
(e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
(f) **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in UK GDPR and the Data Protection Act 2018.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include, but are not limited to:

(a) The individual (or their parent/carer) had given consent.

(b) The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.

(c) The data needs to be processed for reasons of substantial public interest as defined in legislation.

9. Rights of individuals

All individuals are entitled to specific rights under UK GDPR. The school will respond to all Individual rights requests within the permitted timescale.

(a) The right to be informed – the school will provide clear and accessible information about how we process our data via our school Privacy Notice, which can be found on our website.

(b) The right of access – the school will provide individuals with access to their personal data via a subject access request.

(c) The rights to rectify, erase or restrict processing of their personal data (in certain circumstances).

More information about the rights of individuals can be found on the ICO website: Individual rights - guidance and resources | ICO

10. Responding to Subject Access Requests (The 'right of access')

The school will process all subject access requests within one month of receipt, and provide a copy of the information free of charge.

If requests are complex or numerous the school has the right to extend the timescale for the response by up to a further two months. The school will notify the request applicant if this occurs.

If a request could be deemed 'manifestly unfounded or excessive' the school has the right to refuse the request. If we do so, we will notify the individual and explain why the request has been refused.

Parents, or those with parental responsibility, also have a legal right to access to their child's curricular and educational record (as defined with the Education Pupil Information (Wales) Regulations 2011) within **15 school days** of receipt of a written request.

11. Data Security

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.

For example, we will ensure that paper records containing personal data are stored securely (e.g. in locked cabinets) and are not left in accessible locations; that our laptops are password-protected, and that encryption software is used on all portable devices.

12. 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 the school's Data Security Incident procedures. All data security incidents will be referred to the Schools DPO for review.

When appropriate, the Schools DPO will report the data breach to the ICO within 72 hours after becoming aware of it.

13. Storage and retention of personal data

The school will not retain any personal data for any longer than is necessary. The length of time over which data should be retained will depend on the circumstances, including the reason why the personal data was obtained. The school will follow the Schools Retention Schedule guidance which sets out the relevant retention period.

Personal data that is no longer required will be deleted permanently from our records and any hard copies will be destroyed securely.

14. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's data protection rights (for example if the school is planning to use a new form of technology) we will look to conduct a DPIA, in order to assess any potential risks to individuals, to confirm whether the processing is necessary and proportionate, and to identify measures that can be put in place to address any risks.

The DPIA will be carried out with the assistance of the Schools Data Protection Officer.

15. Sharing personal data

The school will not share personal data with any third party without an appropriate legal basis to do so. Examples of when we may do so include:

(a) If we have specific parental consent to do so – for example, sharing a child's photo to a media outlet.

(b) If it is necessary for the performance of our Public Task.

(c) If we need to share with a contractor or supplier. If we do this we will only appoint such third parties that can provide sufficient guarantees that they will comply with data protection law. Data shared will be kept to the minimum required to carry out the relevant service. We will ensure that a suitable contract /data sharing agreement is in place.

(d) If we have to share data with emergency services in the event of an emergency.

(e) If we are legally required to do so with law enforcement or government bodies – for example, to assist with crime prevention and detection, or for safeguarding purposes.

16. 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 and relevant Wrexham County Borough Council documents 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 office.

17. Biometrics

The school do not use any biometric systems within the school premises.

18. Artificial Intelligence

The school will not enter any personal information into any unauthorised generative AI tools. If the school were to accidentally do this, it would need to be reported as a data breach in line with the school's Data Security incident procedure.

19. Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities. This will be mandatory for all staff. Individuals whose roles require regular access to personal data, for example those responsible for responding to subject access requests, may receive additional training to help them understand their duties and how to comply with them.

20. Complaints

Any complaints about the way in which the School deals with personal information will be dealt with by the Governing Body who will arrange for the matter to be investigated. If the complainant is dissatisfied with the outcome of the investigation by the school, they may complain directly to the Information Commissioner. Appeals against the decision of the Information Commissioner can be made to the Information Tribunal at:

Information Commissioner's Office – Wales
2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Tel: 0330 414 6421

wales@ico.org.uk

21. Review and monitoring arrangements

This policy will be reviewed every three years and approved by the full governing body.