Cefn Saeson Comprehensive School
Ysgol Gyfun Cefn Saeson

Data Protection Policy
2025-26

Headteacher	Miss C Jones
Chair of Governors	Mr S John
Date of Review	Autumn 2026

Neath Port Talbot Council
Schools Information Governance Service

1 Introduction

In order to operate efficiently the School has to collect and use information about people with whom it works and the pupils it provides an education to. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with legal obligations and requirements for the provision of education.

The School is committed to ensuring personal data is properly managed and that it ensures compliance with current data protection legislation. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

The School, and any person who handles personal data on behalf of the school (including all staff) must comply with this policy and in particular, the data protection principles in order for the School to comply with the applicable law.

2 Scope

This policy applies to all employees, governors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the School.

This policy applies to all personal data created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive, or HWB SharePoint filing structure, workbooks, email, filing cabinet, shelving and personal filing drawers).

Personal data is information about living, identifiable individuals, or an identifier or identifiers that can be used to identify a living individual. It covers both facts and opinions about the individual. Such data can be part of a computer record or manual record.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

This policy should be read in conjunction with the School's other policies and procedures relating to data protection, including any relevant Privacy Notices, the Data Breach Policy, the Access Control Policy, Record Management Policy and the Guidance on how to handle Subject Access Requests in Schools.

3 Roles and Responsibilities

Overall responsibility for ensuring that the School meets the statutory requirements of any data protection legislation lies with the Governors and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Headteacher.

The Headteacher is responsible for ensuring compliance with data protection legislation and this policy within the day-to-day activities of the School. The Headteacher is responsible for ensuring that appropriate training is provided for all staff.

All contractors who hold or collect personal data on behalf of the School by way of written contract are responsible for their own compliance with data protection legislation and must ensure that personal information is kept and processed in line with data protection legislation and only upon instruction from the school, via a contract.

4 The Requirements

Data protection legislation stipulates that anyone processing personal data must comply with principles of good practice; these principles are legally enforceable. The 6 data protection principles require that personal data:

1. Shall be processed fairly and lawfully and transparently;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;

Shall be kept secure i.e. protected by an appropriate degree of security;

In addition:

- the School is responsible for and must be able to demonstrate compliance with the data protection principles listed above.
- the data shall be processed in accordance with the rights of data subjects. (See Section 9.)

Personal data shall also not be transferred to a country unless that country or territory ensures an adequate level of data protection or another secure method of transfer is guaranteed.

5 Notification

The school, as a Data Controller, is required to notify the Information Commissioner's Office (ICO) and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of Data Controllers, in which the School must be registered. The School will review the Data Protection Register annually, prior to renewing its notification to the Information Commissioner, (https://ico.org.uk/esdwebpages/search).

6 Privacy Notices

Whenever information is collected about individuals they must be made aware of the following at that initial point of collection:

- The identity of the Data Controller, e.g. the School;
- Contact details of the Data Protection Officer;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- What the lawful basis is for processing the data;
- Who the information will or may be shared with;
- If the data is transferred outside of the UK, and if yes, how is it kept secure;
- How long the data will be kept for; and
- How data subjects can exercise their rights.

The School will review its Privacy Notice annually and alert pupils and parents to any updates.

7 Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the UK GDPR has been satisfied.
Processing of special category (sensitive) personal data may only be carried out if a condition in Article 9 of the UK GDPR is met as well as one in Article 6. The School will ensure that all processing meets these requirements.

8 Data Protection Officer

The School shall appoint a Data Protection Officer in line with the requirements of the UK GDPR.

9 Data Protection Impact Assessments

The School shall undertake Data Protection Impact Assessments in line with the requirements of the UK GDPR and as per the Information Commissioner's Office (ICO) guidance.

10 Data Breaches

All employees, governors, contractors, agents and representatives, volunteers and temporary staff must immediately report a security incident or data breach to the Headteacher in accordance with

the Data Breach Policy. The School shall report any personal data breach to the ICO in line with the requirements of the UK GDPR.

11 Contracts

The School shall ensure that a legally binding contract is in place with all of its Data Processors in line with the requirements of the UK GDPR. Before entering into these arrangements, the School will ensure that due diligence is undertaken and appropriate data processing conditions are in place to meet its obligations under Article 28 of the UK GDPR.

12 Consent

Where the School processes data with consent (for example, to publish photographs of children, to send direct marketing emails about school uniform for sale) it will ensure that the consent is freely given, specific, informed and unambiguous, and the consent is recorded.

13 Direct Marketing

Where the School sends any direct marketing (the promotion of aims and ideals as well as selling goods and services) via electronic communications e.g. email, SMS text, fax or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them e.g. has ticked a box to 'opt in'. The School will keep a record of such consent in order to comply with the legislation and the right for consent to be withdrawn.

14 Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Other members of staff on a need to know basis;
- Relevant Parents/Guardians;
- Other authorities if it is necessary in the public interest, e.g. prevention of crime, safeguarding;
- Other authorities, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements.

The School should not disclose anything on a pupil's record which would be likely to cause harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records. Where there is doubt, or statutory requirements conflict, legal advice should be obtained. Where there are safeguarding concerns, the matter should be referred to the School's Safeguarding Lead. When giving

information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. Care must always be taken when there is any doubt about parental responsibility.

15 The Individual's Rights

Under the General Data Protection Regulations 2018, an individual has the following rights which they can exercise in relation to the information the School holds about them. They are entitled to a copy of that information, to see if the data held are accurate, and who it is shared with amongst others. There are exemptions and restrictions that can, in some circumstances, be legitimately applied to exempt or qualify the right of individuals to exercise their rights.

When any request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month and in some instances, for education records, 15 school days under The Pupil Information (Wales) Regulations 2011.
All staff must recognise and log such a requests immediately with the Headteacher. For requests from individuals to access their information, please refer to the School's Guidance on how to handle Subject Access Requests in Schools for further details.

16 Provision of Data to Children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis. If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response. Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

17 Parents' Rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child. The School has the right to ask the Child if they object to release of information to the Parent if the Child is deemed mature enough to make such a decision.

In addition, parents have their own independent right under The Pupil Information (Wales) Regulations 2011 of access to the official education records of their children.

18 Information Security

All members of staff should be constantly aware of the possibility of personal data being seen or accessed by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. All removable devices e.g. laptops, USB sticks, personal mobile phones and digital cameras must not be used to store School data unless they are encrypted and complex password protected wherever possible. Staff and visitors are not permitted to use their own devices in school unless they have the permission from the Headteacher.

All members of staff should take care when transporting paper files between sites. No personal data is ever to be left unattended off site e.g. in a car overnight, on view to family members when working at home.

All members of staff should take care when emailing personal data, checking the email address is correct and the right attachment has been included and that the information is appropriately protected. When copying an email to several people externally, all members of staff should always use the BC field and not the CC field or create a group.

19 Maintenance of Up-to-Date Data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined. In line with UK GDPR requirements the School has a Records Management Policy supported by a Retention Schedule to clarify the retention and disposal of information.

20 Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the

information. This must be answered within one month. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. The School will work with the person to correct the data or allay their concerns. If not satisfied an individual is entitled to apply to the Court for a correcting order.

21 Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous, factual and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent unless it is a legal requirement (e.g. Governors' details). At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

22 Photographs

Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

23 Breach of the Policy

Non-compliance with the requirements of data protection legislation by members of staff could lead to serious action being taken by third parties against the School. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal without notice. It should be noted that an individual can commit a criminal offence under the law, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the Data Controller.

24 Further Information

Further advice and information about data protection legislation, including full details of exemptions, is available from the ICO website at www.ico.org.uk, or from Neath Port Talbot Council's Risk and Information Governance Team. Email igt@npt.gov.uk.

25 Review of the Policy

This policy is to be reviewed bi-annually.

Adopted by Chair of Governors on 11th November 2025
Chair of Governors Mr S. John

Appendix A: Glossary

Data Controller	Data Controller A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Subject	The individual who the data or information is about.
Data Subject Request	A request from a Data Subject to exercise their rights under the General Data Protection Regulations.
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the pupil or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
UK GDPR	The provisions of the EU General Data Protection Regulations as incorporated directly into UK law as the UK GDPR.
Information Commissioner	The independent regulator who has responsibility to see that the data protection legislation is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the law.
Notified Purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing. Just holding or storing the data constitutes processing.
Processed fairly and lawfully	Data must be processed in accordance with the provisions of data protection legislation. These include the data protection principles, the rights of the individual and notification
Special Category (sensitive) Data	Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, or biometric or genetic data.
Subject Access Request	An individual's request for personal data under the General Data Protection Regulation.