Brynnau Primary School

Ysgol Gynradd Brynnau

POLICY: Data Protection Policy

2024 - 2025

'Helping each other to succeed'
'Helpu ein gilydd i lwyddo'

Data Protection Policy

Date	Review Date
October 2024	October 2025

Data Protection Act

Schools like any other organisation, are subject to the Data Protection Act (DPA) and its eight basic principles. The DPA refers to 'personal data' – this can be described generally as information which identifies an individual and is personal to an individual.
The DPA contains eight 'Data Protection Principles' which specify that personal data must be:

- Processed fairly and lawfully
- Obtained for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept any longer than necessary
- Processed in accordance with the 'data subject's' (the individual's) rights
- Securely kept
- Not transferred to any other country without adequate protection

Aims

- To make all staff aware of the need for confidentiality and safekeeping of data in line with the Data Protection Act.

Procedure

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.
It is the responsibility of **all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:**

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the local authority).

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the "Privacy notice" and lawfully processed in accordance with the "Conditions for processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including learners, members of staff and parents/carers, e.g., names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records, e.g., employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior information risk officer (SIRO) and Data Protection Officer is Mrs. Beth Atkin (Headteacher). The Headteacher will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information asset owners (IAOs)

The school will identify Information asset owners (IAOs) is Mrs. Rebecca Price who will monitor the for the various types of data being held (e.g. learner, staff, information, assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a governor.

Registration

The school is registered as a Data controller on the Data protection register held by the Information Commissioner:
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to parents and carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents and carers of all learners of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties, (e.g., LA, etc.) to whom it may be passed. This privacy notice will be passed to parents and carers through Teams, the school website and school newsletter. Parents/carers of young people who are new to the school will be provided with the privacy notice through the school website and prospectus. More information about the suggested wording of privacy notices can be found on the Welsh Government website.

Training & awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through: (schools/colleges should amend or add to as necessary)

- induction training for new staff
- staff meetings/briefings/Inset
- day to day support and guidance from Information asset owners (or insert titles of relevant persons)

Risk Assessments

Information risk assessments will be carried out by Information asset owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences); and
- prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (See Appendix 1):

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools/colleges
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g., the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.
All documents (manual or digital) that contain protected or restricted data will be labelled clearly and passwords applied or classification placed in the footer.
Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts learners at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.
Release and destruction markings should be shown in the footer, e.g., "Securely delete or shred this information when you have finished using it".

Secure storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
All users will use strong passwords which must be changed regularly (see School Password Security Policy). User passwords must never be shared.
Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be **locked if left (even for very short periods) and set to auto lock if not used for five minutes.**

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
Personal data can only be stored on school equipment, this includes computers and portable storage media.
Private equipment (ie owned by the users) must not be used for the storage of personal data.

Headteacher:		*Date:*	*October 2024*
Chair of Governors		*Date:*	*October 2024*

Appendix 1

Information Risk Actions Form

Risk ID	***Information asset affected***	***Information asset owner***	***Protective marking (Impact level)***	***Likelihood***	***Overall risk level (low, medium, high)***	***Action(s) to minimise risk***