



Appropriate Policy Document (APD) (Ysgol Golwg Pen y Fan)

Version:	1
Date Issued:	03.03.25
Date of Previous Issue:	N/A
Approved by:	Governing Body
Date Approved:	03.03.25
Review Date:	03.03.27

Signatures:

	Name	Signature
Chair of Governors:	Jess Williams	<i>J. Williams</i>
Headteacher:	Sarah Court	<i>S. Court</i>

Document Control:

Organisation	Ysgol Golwg Pen y Fan
Title	Appropriate Policy Document (APD)
Author	Professional Lead - Data Protection (Powys County Council)
Owner	Ysgol Golwg Pen y Fan
Subject	Information Governance (IG) Policy
Protective Marking	No protective marking
Version	1
Review Date	August 2024

Revision History:

Revision Date	Revision	Previous Version	Description of Revision
V0.1/0.2/0.3	Draft	N/A	Development of draft
V1	Final	Draft 0.3	Final amendments

Policy Contents:

1. Policy Statement.
2. Scope.
3. Definition of Special Category and Criminal Offence Data.
4. Schedule 1 Conditions for Processing Special Category and/or Criminal Offence data.
5. Procedures for Ensuring Compliance with Data Protection Principles.
6. APD Review Date.

1. Policy Statement:

The Data Protection Act 2018 ('DPA 2018') requires that the controller has an "Appropriate policy" document (APD) in place when processing special category and criminal offence data ('SC/CO') under reliance on Schedule 1 Part 1, 2 & 3 of the DPA 2018.

Schedule 1 Part 4 (paragraph 38) makes the provision about the "processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of this schedule [DPA 2018] which requires the controller to have an appropriate policy in place when the processing is carried out".

This policy sets out Ysgol Golwg Pen y Fan's response to this obligation. It indicates how the School as the controller processes SC/CO data in compliance with the UK GDPR Article 5 principles.

This APD supplements the school's privacy notice.

2. Scope

The school processes SC/CO data in certain circumstances when providing services to its students, parents or guardians of those students, staff, and/or customers, based on some of its duties and obligations as a Public Authority and employer.

SC/CO data is processed in reliance of conditions within Articles 9 and 10 of the UK GDPR in addition to those conditions set out in Schedule 1 Part 1, 2 & 3 of the DPA 2018.

This APD does not cover the processing of SC/CO data for the purposes of law enforcement, which is carried out by the school as a competent authority but falls under Part 3 of the DPA 2018.

3. Definitions of Special Category and Criminal Offence Data:

Article 9 of the UK GDPR defines special category data as personal data which reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Health data;
- Data concerning a natural person's sex life or sexual orientation.

Section 11 (2) of the DPA 2018 defines criminal offence data as personal data relating to criminal convictions and offences or related security measures, relating to:

- The alleged commission of offences by the data subject, or;

- Proceeding for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

4. Schedule 1 Conditions for Processing Special Category and/or Criminal Offence data:

The different conditions for processing SC/CO data within Schedule 1 are listed below.

Schedule 1 Part 1 – Conditions relating to Employment, Health (& Research):

For the purposes of carrying out employer-related obligations in connection with rights under employment law.

For the purposes of carrying out an assessment of the working capacity of an employee.

Schedule 1 Part 2 – Conditions relating to Substantial Public Interest:

Equality of Opportunity or Treatment:

For the purposes of ensuring compliance with obligations under legislation such as the Equality Act 2010.

Racial and Ethnic Diversity at Senior Levels of an Organisation:

For the purposes of identifying suitable individuals to hold senior positions within the school.

Preventing or Detecting Unlawful Acts:

For the purposes of carrying out enforcement action as per our statutory duties.

Regulatory Requirements relating to Unlawful Acts & Dishonesty:

For the purposes of assisting other Authorities in connection with their regulatory requirements.

Preventing Fraud:

For the purposes of processing in accordance with arrangements made by anti-fraud organisations.

Counselling:

For the purposes of providing counsel, advice or support or of another similar service provided confidentially.

Safeguarding of Children and Individuals at Risk:

For the purpose of protecting vulnerable children and or individuals over the age of 18 from neglect, physical, mental, or emotional harm.

Insurance:

For the purposes of responding to claims for compensation made against the School.

Disclosure to Elected Representatives:

For the purposes of assisting Local County Councilors with requests for assistance on behalf of their constituents.

Schedule 1 Part 3 – Additional Conditions Relating to Criminal Convictions etc.:

The school may process personal data where it is strictly necessary for law enforcement purposes, and it meets the relevant conditions in the DPA 2018.

5. Procedures for Ensuring Compliance with Data Protection Principles**The First Principle: Article 5 (a) – Lawfulness, fairness & transparency.**

SO/CO data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The school shall ensure that the processing of SO/CO data is lawful by identifying one or more of the six legal bases provided in Article 6 of the UK GDPR, as well as a condition under Article 9 (or 10) of the UK GDPR, and, where appropriate, a condition under Schedule 1 of the DPA.

A large proportion of the school's processing activities are carried out in conjunction with Article 6 (c) and (e): a legal obligation and public task, respectively, and Article 9 (b) and (g): obligations of the controller and substantial public interest, respectively.

The school shall ensure transparency by providing, when appropriate, and when an exemption does not apply, privacy information to any data subject to which the personal data being processed belongs to. This is known as a privacy notice.

Processing personal data fairly encompasses the above points, and the school further achieves fair processing by ensuring all forms of processing are assessed, especially forms of high-risk processing, which are assessed through Data Protection Impact Assessments (DPIA).

The Second Principle: Article 5 (b) – Purpose Limitation

Personal data shall be collected for a specified, explicit, and legitimate purpose.

Special category and criminal offence data shall only be collected in order to fulfill statutory obligations in accordance with relevant legislation and the school will ensure that the data will then not be processed for purposes incompatible with the original purposes for which it was collected.

Proper consideration will be given to secondary processing compatibility with the original purpose.

The Third Principle: Article 5 (c) – Data Minimisation

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

The school will only collect and process SC/CO data which is relevant to the purpose of processing.

The Fourth Principle: Article 5 (d) – Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

The school will take every reasonable step to ensure that personal data identified as being inaccurate is rectified or erased without delay.

The Fifth Principle: Article 5 (e) – Storage Limitation

SC/CO data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The school will retain this information in accordance with its retention schedule and will delete or archive SC/CO that is no longer required.

It may be stored longer solely for archiving purposes in the public interest. (Archives provide first-hand information or evidence relating to historical events or figures)

The Sixth Principle: Article 5 (f) – Integrity and Confidentiality (Security)

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.

Digital SC/CO data is only processed through systems that comply with appropriate security standards. Hard copy documents containing SC/CO are governed by other policies.

The Seventh Principle: Article 5 (2) - Accountability

The school have put in place, measures to meet the requirements of accountability under the UK GDPR and will maintain these under continual review.

This includes (but is not limited to):

- The appointment of a Data Protection Officer (who reports directly to Powys County Council's highest management level);
- Adopting and implementing data protection policies and ensuring written contracts/agreements are in place between the Council's processors.
- Carrying out Data Protection Impact Assessments (DPIA), where required.
- Ensuring that staff have completed Cyber Security and UK GDPR training.

6. APD Review Date:

This policy will be retained for the duration of the school's processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed every 2 years or revised more frequently if necessary.