Ysgol Gynradd Gymraeg Gorslas Data Protection Policy



sirgar.llyw.cymru
carmarthenshire.gov.wales

Cyngor Sir Gâr
Carmarthenshire
County Council

School Data Protection Policy

Contents

1. Data Protection legislation and personal data
2. Special category personal data
3. The supplementary requirements of the Data Protection Act 2018
4. Purpose of this Policy and its scope
5. How we comply with the principles
6. Retention and erasure of personal data
7. Ensuring equality of treatment
8. Rights of access to information
9. Process for handling a subject access request (SAR)
10. Complaints
11. Contacts

1. Data Protection legislation and personal data

1.1 The School collects and uses personal data relating to our customers, clients, employees and residents within the County in order to provide its wide range of services. In doing so, the School is committed to complying with the requirements of Data Protection legislation across all of its services. For the purposes of this Policy, this legislation is comprised of:

- The UK General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA)

1.2 Personal data is defined as any information relating to an identifiable person who can be identified directly or indirectly by referring to an 'identifier'. In practice, a wide range of identifiers or items of information will constitute personal data, including names, addresses, unique reference numbers, online identifiers and even narrative about a person.

1.3 The GDPR sets out six principles relating to the processing of personal data. These are:

- Personal data must be processed lawfully, fairly and transparently
- Personal data must be collected for specified, explicit and legitimate purposes, and other uses must be compatible with these purposes
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is used
- Personal information must be kept accurate and where necessary, up to date
- Personal data must not be kept for longer than is actually necessary
- Personal data must be processed in a secure manner, including protection against unauthorised or unlawful use of personal data and against its accidental loss, destruction or damage, using appropriate technical and organisational measures

1.4 The School is committed to complying with the legislation by applying these principles across all its services.

1.5 The GDPR also prohibits the School from processing personal data unless we are able to identify an appropriate legal basis for that processing.

1.6 In the main, the processing of personal data carried out by the School is carried out on the following lawful bases:

- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the School; or
- To comply with our legal obligations.

2. Special category personal data

2.1 The GDPR also requires us to meet special conditions for processing special category personal data and criminal convictions data. The GDPR prohibits the processing of this kind of data unless the special conditions can be met.

2.2 The special categories are personal data about:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

2.3 The special conditions which allow processing of special category personal data include:

- Article 9(2)(b) – for employment, social security and social protection purposes
- Article 9(2)(g) – for substantial public interest purposes
- Article 9(2)(h) – for health and social care purposes
- Article 9(2)(i) – for public health purposes
- Article 9(2)(j) – for archiving, research and statistics purposes
- Article 10 also requires that the processing of criminal convictions data is prohibited unless it is carried out under the control of official authority or if it is authorised by UK law

2.4 The GDPR allows the United Kingdom and member states of the European Union to supplement these provisions regarding the processing of special category and criminal conviction data, and these are found in the DPA.

3. The supplementary requirements of the Data Protection Act 2018

3.1 Section 10 and Schedule 1 of the DPA set out the exceptions from the prohibitions in the
GDPR relating to processing the special categories of personal data and criminal convictions data.

3.2 Along with other conditions in Schedule 1, Part 1 of the DPA, the School relies on the
following in relation to the processing special category personal data:

- Employment, social security and social protection - processing necessary for the purposes of performing of exercising obligations or rights of the School or the data subject under employment law, social security law or the law relating to social protection.

3.3 The School also processes special category personal data under the following conditions in Schedule 1, Part 2 of the DPA, on grounds of substantial public interest:

- Statutory and government purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Preventing fraud
- Counselling, advice or support services
- Insurance purposes
- Occupational pensions
- Elected representatives responding to requests
- Disclosure to elected representatives

3.4 Criminal convictions data is defined as information about criminal allegations, proceedings or convictions.

3.5 Along with other conditions in Schedule 1, Part 3 of the DPA, the School also extends the statutory and government purposes condition found in Part 2 to process criminal convictions data.

3.6 In order to extend this condition to process criminal convictions data, the School must meet the substantial public interest test.

3.7 The School considers this test is met on the following grounds:

In all the circumstances of each processing activity, the public interest in the processing of the criminal conviction data substantially outweighs the public interest in preserving the privacy of the data subject.

This is clearly the case where data subjects themselves derive benefits from the processing of the data and where the processing is necessary and proportionate in order to protect the general public, including children and vulnerable adults.

The School keeps records of all services which process criminal conviction data and in each case, we document the public interest factors relied upon to outweigh privacy issues.

4. Purpose of this Policy and its scope

4.1 To apply any of the conditions referred to under sections 3 and 4 of this Policy, the School must have in place an appropriate policy document which explains:

- How we comply with the six data protection principles set out in the GDPR; and
- Our policies for the retention and erasure of personal data processed under these conditions.

4.2 This purpose of this Policy is therefore to comply with these specific legal requirements in relation to the processing of special category personal data and criminal convictions data by the School. However, the measures and actions taken to comply with the principles apply equally to all personal data held by the School.

4.3 This policy applies to all employees of the School, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

5. How we comply with the principles

5.1 Principle 1 – lawfulness, fairness and transparency

- Privacy notices are in place for all services which process personal data, including special category and criminal convictions data. These notices make clear that special category and criminal convictions data are being processed and set out the lawful basis for processing of this personal data.

- These privacy notices are published prominently on the School website, are provided to the public when personal data is collected from them and are referred to in other communications.

- Further detail on how personal data is processed is set out in the School's Privacy Notice.

Ysgol Gynradd Gymraeg Gorslas - Polisiau / Policies

5.2 Principle 2 – purpose limitation

- Our privacy notices and records of processing activities clearly set out the purposes for which the personal data is processed and identify the lawful basis for the processing. These are regularly reviewed in consultation with the School Data Protection Officer.

5.3 Principle 3 – data minimisation

- Managers and Information Asset Owners are subject to a training programme which specifies their obligation to only process the personal data which is required for their specific business function.

- Periodic reviews of the personal data held in individual business units are undertaken and data which is no longer needed is deleted, in accordance with the School's Retention Guidelines.

- Compliance with this principle will be subject to Internal Audit review.

5.4 Principle 4 – accuracy

- Where appropriate, School services have in place review mechanisms to check that personal data remains accurate and up to date.

- Individuals are informed of their right to rectification and we carefully consider any requests received to exercise this right. We keep records of such requests from individuals.

- Managers and Information Asset Owners are subject to a training programme which specifies their obligation to regularly review, update and correct personal data.

- Compliance with this principle will be subject to Internal Audit review.

5.5 Principle 5 – storage limitation

- The School has in place a Records Management Policy which requires that detailed Retention Guidelines are in place covering all its services, including those that process special category and criminal convictions data**.** These are based on legal requirements to retain personal data for specific periods as well as the identified need of each business unit.

- The School will utilise software which will automatically apply a retention period to personal data upon its creation, in accordance with the Retention

Guidelines, and which will subsequently delete or review the personal data that has reached its retention period.

- Other systems and databases are regularly reviewed and personal data is deleted where it has passed its retention period.

5.6 Principle 6 – integrity and confidentiality (security)

Organisational measures

- The School has in place clear policies and procedures which require that staff keep personal data secure and provide information on how to do so:

    - Information Security Policy
    - School Privacy Notice
    - Handling Personal Information Policy & Procedure
    - Breach Reporting & Response Policy - Personal data breaches will be reported and managed in accordance with the School's Breach Reporting Policy, including reporting to the ICO where required under Article 33 UK GDPR.

- These are regularly reviewed, actively communicated to employees and made available for reference on the School's SharePoint site.

- The School has in place a training programme which places an emphasis on data security.

- All personal data is processed in buildings protected from public access by swipe card entry systems.

- Personal data processed in paper format is kept in lockable storage within these areas.

  The School ensures that all external processors implement appropriate technical and organisational measures, operate under a written contract, and only process personal data on documented instructions, in compliance with Articles 28 and 32 of UK GDPR.

  Where processing is likely to result in a high risk to individuals' rights and freedoms, the School will undertake a Data Protection Impact Assessment (DPIA) prior to processing, in accordance with Article 35 of UK GDPR.

Technical measures

- Data is stored in secure data centres. Controls are in place to prevent unauthorised access to buildings and only authorised personnel may

access these data centres. Any contractors permitted access are supervised.

- A perimeter firewall controls connections between the School's internal network and the internet. It is used to restrict bi-directional communications to only what is required, to prevent unauthorised access from the internet and to prevent unauthorised outbound transfer of data.

- Where it is a requirement under the above policies to do so, personal data sent to external parties is encrypted. Only authorised solutions are used.

- Access rights to data is managed on a per user basis and permissions to data sources are granted only when there is a requirement. Access is revoked when the requirement expires.

- Servers and applications are kept up to date to prevent the exploitation of known vulnerabilities that could have a negative impact on the confidentiality, integrity and availability of data. There is also anti-malware software running on all endpoint devices and at the internet gateway.

- The network is penetration tested regularly to identify and subsequently remediate any vulnerabilities to ensure the protection of data.

- A multi-layered approach to security is in place to provide a resilient defence against cyber-attacks and protection for the data we hold.

- All core systems are backed up to prevent loss of data and for recovery in the event of a disaster.

6. Retention and erasure of personal data

6.1 The School manages its records in line with its retention schedule, developed with reference to the IRMS Schools' Toolkit, which specifies the retention periods for different categories of records and the requirements for their subsequent secure disposal.

6.2 Where not specified, special category and criminal conviction data are included within other record types.

6.3 Erasure or destruction of personal data is carried out in accordance with our Records Management Policy.

7. Ensuring equality of treatment

7.1 This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

8. Rights of access to information

There are two distinct rights of access to information held by Schools about pupils.

1. Under Article 15 of UK GDPR, data subjects have the right to access information held about them by the school and to have a copy of that personal data.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

9. Process for handling a subject access request

1. Requests can be made verbally or in writing, including by email. admin@gorslas.ysgolccc.cymru
2. If the initial request does not clearly identify the information required, then further enquiries will be made.

3. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement *This list is not exhaustive*.

4. Any individual has the right to access personal data held about them. In the case of children, this right depends on their capacity to understand the nature of the request. This will be assessed on a case-by-case basis, taking into account the child's level of maturity and understanding (often considered to be from around age 12, but not applied as a fixed rule). The Headteacher should, where appropriate, discuss the request with the child and take their views into account when making a decision.

5. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The School may charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

5. The response time for subject access requests, once officially received, is one month **(irrespective of school holiday periods)**. One month time limit should be calculated from the day after the SAR is received until the corresponding calendar date in the next month. This meant that if the SAR was received on 19 August 2025, the response deadline would be 20 September 2025. UK GDPR and Data Protection Act 2018 allows schools to pause the one month response deadline if clarification is required to process the request (e.g., overly broad requests). The clock resumes once the requester responds.

The school can extend the time to respond by a further two months if the request is:

- complex; or
- you have received a number of requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another School. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the one month statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information, then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the School with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

10. Complaints

1. If you have any concerns about how the school handles your personal data, you have the right to make a complaint. We encourage you to raise any concerns with us in the first instance so that we have the opportunity to investigate and resolve the issue. You can do this by contacting: admin@gorslas.ysgolccc.cymru

We will acknowledge your complaint within 30 days and will aim to investigate and respond without undue delay. We will keep you informed of the outcome and any actions taken.

If you are not satisfied with our response, or if you believe we have not handled your complaint appropriately, you have the right to lodge a complaint with the Information Commissioner's Office (ICO): Information Commissioner's Office Telephone: 0303 123 1113

11. Contacts

1. If you have any queries or concerns regarding these policies / procedures then please contact admin@gorslas.ysgolccc.cymru

For further information about your data protection rights, please refer to the ICO's guidance on individuals' rights under UK GDPR. see the guidance from the UK Information Commissioners Office (ICO)

Cytunwyd ar ran y llywodraethwyr gan/ Agreed on behalf of the governing body by – (Enw/Name) Shan Thomas	Arwyddwyd/Signed: Shan Thomas Dyddiad/Date: Medi 2026
Arwyddwyd gan y Pennaeth/ Signed by Headteacher Angharad Vaughan-Owen	EA Vaughan-Owen Dyddiad/Date: Medi 2026
Adolygiad nesaf/Review date:	Medi 2027