



Data Breach Procedure Policy

Written	January 2026
Author	Sam Thomas
Role	Headteacher
Last Review	January 2026
Review Date	January 2027

Purpose of this procedure

This procedure sets out how Ysgol Y Rhos identifies, manages, investigates and reports personal data breaches involving pupil, parent and carer data.

It ensures that data breaches are handled promptly, effectively and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, Welsh safeguarding guidance and regulatory expectations.

This procedure applies only to personal data processed by Ysgol Y Rhos relating to pupils, parents and carers. Breaches involving employee data are managed under a separate procedure.

What is a personal data breach?

A personal data breach is a security incident that leads to the accidental or unlawful:

- Destruction of personal data
- Loss of personal data
- Alteration of personal data
- Unauthorised disclosure of personal data
- Unauthorised access to personal data

Personal data breaches can involve paper records, electronic systems, emails, images, CCTV or verbal disclosures.

Examples of data breaches

Examples of data breaches include, but are not limited to:

- Sending pupil information to the wrong recipient
- Loss or theft of a laptop, USB device or paper file containing personal data
- Unauthorised access to safeguarding or SEN records
- Accidental disclosure of personal data in emails or reports
- Hacking, malware or ransomware attacks
- Inappropriate sharing of information verbally or electronically

Reporting a data breach

All staff, volunteers and contractors working within Ysgol Y Rhos have a responsibility to report any actual or suspected data breach immediately.

Breaches must be reported as soon as possible to:

- The Data Protection Lead, Sharon Kettlewood – HR Manager
- A member of the Senior Leadership Team

If a breach involves safeguarding or child protection information, the Designated Safeguarding Person must also be informed without delay.

Staff must not attempt to investigate or resolve breaches themselves.

Immediate Containment Actions

Upon becoming aware of a data breach, Ysgol Y Rhos will take immediate steps to contain and minimise the breach. This may include:

- Retrieving wrongly sent information
- Shutting down compromised systems
- Securing lost or stolen devices (where possible)
- Changing passwords or access permissions
- Isolating affected systems

All actions taken must be recorded.

Investigation of the breach

The Data Protection Lead will coordinate an investigation to establish:

- What happened and how the breach occurred
- The type and volume of personal data involved
- Whether special category or safeguarding data is affected
- The number of individuals affected
- The potential risks to the rights and freedoms of individuals

The investigation will also consider whether safeguarding concerns arise as a result of the breach.

Assessing risk and harm

Ysgol Y Rhos will assess whether the breach is likely to result in a risk to the rights and freedoms of individuals.

Factors considered include:

- The sensitivity of the data involved
- Whether children are affected
- Whether safeguarding or health data is involved
- The likelihood of further disclosure or misuse
- The potential for emotional, physical or reputational harm

Notification to the Information Commissioners Office (ICO)

The School will notify the Information Commissioner's Office (ICO) of a data breach without undue delay and within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals.

Where notification is required, the School will provide the ICO with:

- A description of the nature of the breach
- The categories and approximate number of individuals affected
- The categories and approximate number of personal data records involved
- The likely consequences of the breach
- The measures taken or proposed to address the breach
- Contact details for the Data Protection Lead

If all information is not available within 72 hours, the School will submit an initial report followed by further information as it becomes available.

Communicating with affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, Ysgol Y Rhos will inform affected parents, carers or pupils (where appropriate) without undue delay.

Communications will:

- Be clear and transparent
- Describe the nature of the breach
- Explain the likely consequences
- Set out steps taken to mitigate risk
- Provide advice on how individuals can protect themselves
- Include contact details for further information

Communication may be delayed or limited where this is necessary to protect a child or prevent further harm.

Safeguarding considerations

Where a data breach involves safeguarding or child protection information, Ysgol Y Rhos will:

- Prioritise the welfare of the child
- Consult the Designated Safeguarding Person
- Consider whether additional safeguarding action is required
- Ensure information sharing does not place a child at further risk

Safeguarding considerations may affect decisions about disclosure and communication.

Recording data breaches

The School maintains a Data Breach Log which records:

- The facts relating to the breach

- The effects of the breach
- Actions taken to contain and mitigate the breach
- Decisions regarding notification
- Lessons learned

All breaches are recorded, regardless of whether they are reportable to the ICO.

Learning and Improvement

Following a data breach, Ysgol Y Rhos will:

- Review the causes of the breach
- Identify any weaknesses in systems or procedures
- Take steps to prevent recurrence
- Update training or policies where required

This policy is reviewed every year as a minimum. However, where there are changes to legislation/guidance or in response to recommendation from any significant incident, review of the policy will take place immediately.

Policy Created By	Sam Thomas	09/01/2026
Policy Approved By	Catrin Jones	12/01/2026