Privacy and confidentiality policy and procedure

Ysgol Y Foel Out of School Club | Revised 24 November 2026

Policy statement

Ysgol Y Foel Out of School Club respects the privacy of children, families, staff and others. This policy applies to all staff, volunteers, students and committee members, including temporary staff. We handle personal information lawfully, fairly, transparently and securely, collecting only what is necessary for the provision of safe childcare and associated administration.

The policy has regard to the UK GDPR and Data Protection Act 2018 (as amended, including applicable provisions of the Data (Use and Access) Act 2025), the Child Minding and Day Care (Wales) Regulations 2010 (as amended), and the 2026 National Minimum Standards, particularly Standards 5 and 6.

Responsibilities and access to information

- The registered provider is accountable for data protection. The Person in Charge (Mrs Napper) is the operational lead for information sharing, supported by the Responsible Individual and committee. The committee will confirm a data protection contact and cover arrangements during absences.
- The club will identify its lawful bases for processing, including additional conditions for special category and criminal offence data where applicable, and provide accessible privacy notices explaining purposes, recipients, retention and individual rights.
- Parents may request information about their own child, subject to the child's rights, safeguarding considerations and the privacy of others. Requests will be discussed privately; third-party information will be protected.
- Staff, volunteers and students may request access to their own personal data. Personnel information is restricted to authorised individuals who need it for their duties.
- Requests to exercise data protection rights are passed promptly to the data protection contact. Subject access requests will normally be answered within one month, subject to lawful extensions or exemptions. Identity and authority will be verified as necessary.

Confidentiality and safeguarding

- Information is shared only with authorised recipients on a necessary and proportionate basis, using a lawful basis. Where appropriate, parents are informed and their permission sought for routine referrals. Consent is not a prerequisite for lawful safeguarding disclosures.
- Where a child may be at risk, staff must follow the safeguarding policy and Wales Safeguarding Procedures without delay. Information may be shared without parental consent where lawful and necessary to protect a child. Reasons and decisions must be recorded.

- Records will be made available to CIW as required by law. Information shared with the school or other agencies must be limited to what is necessary; the club and school are separate organisations and their respective data protection responsibilities must be documented.
- Staff must not discuss confidential matters in public or with unauthorised people. This does not prevent safeguarding reports, protected whistleblowing, reporting to regulators or seeking lawful professional advice.

Secure storage and use

- Paper records must be kept in locked storage with restricted access. Electronic records must be held on approved systems with individual accounts, strong passwords, appropriate access controls, encryption where appropriate and secure backups. Use multi-factor authentication where available.
- Personal information must not be transferred to private email, unapproved cloud services or personal devices. When records need to be transported, use secure arrangements and keep them under authorised control. Verify recipients before sending information.
- Access permissions must be reviewed when roles change or staff leave. Confidential information must not be posted on public social media. Any approved processor must have appropriate contractual and security arrangements.

Photographs, recordings and social media

Only authorised equipment and approved channels may be used to photograph or film children. Obtain and record appropriate parental permissions for optional photography and publication, respect children's wishes, and explain how permissions may be withdrawn. Where images are needed for other lawful purposes, document the appropriate basis. Do not publish identifying or sensitive information without appropriate authorisation. Follow the safeguarding and mobile phone policies.

Personal data breaches

Any loss, unauthorised access, accidental disclosure or other suspected breach must be reported immediately to the Person in Charge and the registered provider's designated contact. Contain the breach, preserve evidence, assess risks and document all breaches and decisions. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness when the breach is likely to pose a risk to individuals' rights and freedoms. Inform affected individuals without undue delay if the risk is high, subject to lawful exceptions. Notify CIW and safeguarding agencies where the relevant notification criteria are met.

Retention and disposal

- Individual children's records must be retained for at least three years after their last attendance, also meeting Regulation 30 and Schedule 3 requirements. Retain records longer where required by law, safeguarding needs, insurance or a documented legal reason.
- Accident records: retain in accordance with the Accident and First Aid Policy (the club's previous policy specified at least 21 years; the revised accident policy should be checked against insurer requirements before adoption). Do not destroy records subject to an investigation, claim or legal hold.
- Maintain a documented retention schedule for children's, safeguarding, employment, financial and charity records. Review it regularly; securely shred paper and securely erase electronic

data and devices when lawful to dispose of them. Do not use ordinary waste or uncontrolled burning.

Training, accountability and concerns

All staff, volunteers and students must read and acknowledge this policy at induction and receive refresher guidance. The committee will check whether the club must pay the ICO data protection fee and maintain its registration where required. Suspected breaches of confidentiality will be investigated fairly under the disciplinary procedure; serious breaches may constitute gross misconduct. Concerns may be raised with the Person in Charge or committee, and individuals may complain to the ICO.

Further guidance and contact details

Club contact: 01352 740197 (school office; ask for Out of School Club).
ICO: ico.org.uk | 0303 123 1113
CIW: 0300 7900 126 | ciw@gov.wales
Welsh Government: www.gov.wales/national-minimum-standards-regulated-childcare
Wales Safeguarding Procedures: safeguarding.wales

Policy approval record

Previous approval / version	8 July 2025
Date revised	24 November 2026
Name / position	Mrs Napper – Person in Charge
Approval authority	Out of School Club Committee (delegated authority)
Date approved	_____
Signature on behalf of provider	_____
Next scheduled review	July 2027

Before adoption: confirm the data protection contact, ICO fee status, privacy notices, school/club information-sharing arrangements and the retention schedule, including accident and safeguarding records.