



Brynteg Tigers Out of Hours Club Confidentiality and GDPR Policy

Approved by: Michelle Firth

Policy Reviewed: September 2026

Next Review Due: September 2027

Responsible Individual / Data Protection Lead: Michelle Firth

1. Policy Statement

Brynteg Tigers Out of Hours Club is committed to protecting the privacy, confidentiality, and rights of all children, families, and staff. We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and CIW National Minimum Standards.

We only collect, store, and share information that is necessary to:

- Provide safe, high-quality childcare
- Meet legal and regulatory obligations
- Safeguard children
- Support staff employment and training

We ensure personal data is handled lawfully, fairly, securely, and transparently.

2. Aims

- Keep personal data safe, secure, accurate, and up to date.
- Be clear and transparent about how personal information is used.
- Only share information when legally required or in a child's best interests.
- Ensure staff understand confidentiality and data protection responsibilities.
- Protect the rights of children, families, and staff under UK GDPR.

3. Legal Framework

This policy follows:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children Act 1989 & 2004
- Social Services and Well-being (Wales) Act 2014
- Care Standards Act 2000 / CIW National Minimum Standards
- Human Rights Act 1998

4. Information We Hold

We may hold the following personal data:

Children

- Full name, date of birth, address
- Parent/carer contact details
- Emergency contacts
- Medical information, allergies, health needs
- Attendance records
- Accident/incident forms
- Behaviour or safeguarding notes (stored separately and securely)

Parents/Carers

- Contact details
- Authorised collectors
- Any relevant information needed to support the child

Staff

- Recruitment information (DBS, references, qualifications)
- Training records
- Employment details
- Emergency contacts
- Performance or safeguarding records (where applicable)

All data is collected for legitimate childcare, safeguarding, employment, or legal purposes.

5. Lawful Bases for Processing

We process personal data under the following lawful bases:

- **Legal obligation** — CIW requirements, safeguarding law, employment law
- **Vital interests** — sharing information to protect a child in an emergency
- **Public task** — delivering regulated childcare
- **Contract** — employment contracts
- **Consent** — photos, sharing information with external professionals
- **Legitimate interests** — internal record keeping, communication with families

Consent is only used when appropriate and can be withdrawn at any time.

6. Data Storage & Security

Paper Records

- Stored in locked filing cabinets in a secure office
- Access limited to authorised staff only

Digital Records

- Password-protected devices
- Secure cloud storage where used
- Access restricted to authorised staff
- Regular backups and security updates

Photos & Images

- Only used for childcare purposes with parental consent
- Not stored on personal devices
- Deleted when no longer needed

CCTV

- Managed in line with data protection law
- Signage displayed clearly
- Footage stored securely and accessed only when necessary

7. Sharing Information

We only share personal data when:

- **Required by law** (CIW, HMRC, HSE)
- **Safeguarding concerns** require sharing with Social Services, Police, or safeguarding partners
- **Parents/carers give explicit consent** (e.g., ALNCo, health visitor)
- **It is in the child's vital interests** (medical emergency)

Information shared is always minimal, relevant, and proportionate.

We do not share information with third parties for marketing or commercial purposes.

8. Confidentiality Expectations

All staff, students, and volunteers must:

- Keep information about children, families, and staff confidential
- Never discuss children outside work or on social media
- Only share information with colleagues who need to know
- Hold conversations privately and respectfully
- Follow safeguarding procedures when confidentiality cannot be maintained

Breaches of confidentiality may result in disciplinary action.

9. Data Retention

We follow statutory retention periods:

- **Children's records:** 3 years after leaving (longer if safeguarding-related)
- **Accident/incident reports:** 3 years, or until the child is 21 if related to injury claims
- **Safeguarding records:** Kept in line with local authority guidance (often long-term)
- **Personnel files:** 6 years after employment ends
- **Financial records:** 6 years
- **Medication records:** 3 years

Data is securely destroyed when no longer required.

10. Rights of Individuals

Parents/carers and staff have the right to:

- Access the personal data we hold
- Request corrections if information is inaccurate
- Request deletion where legally appropriate
- Request restriction of processing

- Object to certain types of processing
- Receive information in a portable format (where applicable)
- Complain to the Information Commissioner's Office (ICO)

Requests must be made in writing to the Responsible Individual.

We respond within one month unless the request is complex.

11. Data Breach Management

A data breach includes:

- Loss or theft of data
- Unauthorised access
- Accidental disclosure
- Technical security failure

If a breach occurs:

1. Staff must report it immediately to the Responsible Individual.
2. The breach will be investigated and recorded.
3. Individuals affected will be informed where appropriate.
4. Serious breaches will be reported to the ICO within 72 hours if required.
5. Measures will be put in place to prevent recurrence.

12. Review & Monitoring

This policy is reviewed annually or sooner if:

- Legislation changes
- CIW provides updated guidance
- A breach or incident highlights the need
- New systems or technologies are introduced