Updated: 18 June 2025
Next Review Due: 18 June 2027
Version: 2.0

Data Protection Policy

Part of the BYO Operations and Administration Policy Suite

Britannia Youth Organisation CIC is a Community Interest Company registered in England and Wales.
Company No. 12515346 | Registered Address: 36 St Joseph's Rd, Ward End, Birmingham, B8 2JU

CONTENTS

1. Legal Framework 1
2. Registration and Fees 2
3. Key Definitions 2
4. Data Protection Principles 3
5. Lawful Bases for Processing 3
6. Consent Management 4
7. Responsibilities 6
8. Data Security 7
9. Safeguarding and Information Sharing 8
10. Data Sharing and Third Parties 9
11. Data Retention and Disposal 9
12. Individual Rights 10
13. Data Breaches 11
14. Digital Platforms and Online Safety 12
15. Complaints and Concerns 12
16. Training and Compliance 13
17. Policy Review and Updates 14

Document Type	Policy
Policy Title	Data protection Policy
Version	2.0
Effective Date	18 June 2025
Review Date	18 June 2027
Owner	Designated Safeguarding Lead
Approved By	Hassan Kingsley, Governor
Cross-References	Safeguarding Policy Framework, Anti-Bullying Policy, Code of Conduct Policy, Code of Behaviour Policy, Organisational Values and Inclusion Framework, Recruitment, Selection and Onboarding Policy, Complaints Policy, Whistleblowing Policy

Introduction

This policy outlines how The Britannia Youth Organisation CIC (BYO) ensures compliance with data protection legislation while protecting the rights of our members, participants, staff, directors, volunteers, and partners. We are committed to being transparent about how we collect, store, and process personal data while maintaining the highest standards of information security.

BYO recognises that effective data protection supports our safeguarding responsibilities and helps build trust with the communities we serve.

Safeguarding Connection: Data protection is integral to our safeguarding framework as outlined in our **Safeguarding Policy Framework, Child Protection Procedures,** and **Adult Safeguarding Procedures.**

1. Legal Framework

Our data protection practices comply with:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018, including Law Enforcement Requirements (Part 3)
- Children and Young Persons Act 2008
- Working Together to Safeguard Children (2023)
- Human Rights Act 1998
- Common Law Duty of Confidentiality

This list is not exhaustive and BYO monitors changes to relevant legislation.

2. Registration and Fees

Under the Data Protection (Charges and Information) Regulations 2018, BYO has been assessed as exempt from paying the ICO registration fee due to our status and the nature of our data processing activities.

ICO Registration Number: [To be inserted if registration becomes required]

3. Key Definitions

Personal Data - Any information that can identify a living person, including names, addresses, email addresses, photographs, and any unique identifiers.

Data Subject - An individual who is the subject of personal data (our participants, members, staff, volunteers, and their families).

Data Controller - BYO, as the organisation that determines how and why personal data is processed.

Data Processor - Any third party that processes personal data on our behalf (such as software providers or contractors).

Processing - Any activity involving personal data, including collecting, recording, storing, using, sharing, or deleting information.

Lawful Basis - The legal reason under GDPR that allows us to process personal data.

Special Category Data - Sensitive personal data including health information, ethnic origin, religious beliefs, and information about criminal convictions.

DSL - Designated Safeguarding Lead, the person with lead responsibility for safeguarding across the organisation.

4. Data Protection Principles

BYO processes all personal data in accordance with the six key principles. Personal data must be:

1. **Processed lawfully, fairly and transparently** - We have clear lawful bases for processing and are open about our activities
2. **Collected for specific, explicit and legitimate purposes** - We only collect data we need for our youth work activities
3. **Adequate, relevant and limited** - We collect the minimum amount of data necessary
4. **Accurate and kept up to date** - We regularly review and update personal information
5. **Kept for no longer than necessary** - We have clear retention schedules and delete data when no longer needed
6. **Processed securely** - We use appropriate technical and organisational measures to protect data

We take accountability seriously and can demonstrate our compliance with these principles.

5. Lawful Bases for Processing

BYO processes personal data under the following lawful bases:

- **Legitimate Interest** - For our core youth work activities, safeguarding, and organisational administration
- **Consent** - For photography, marketing communications, and some voluntary activities
- **Legal Obligation** - For safeguarding reporting and health and safety requirements
- **Vital Interests** - In emergency situations to protect someone's life or wellbeing
- **Public Task** - Where we deliver services in the public interest

For processing special category data (such as health information), we rely on additional conditions including:

- Safeguarding of children and individuals at risk
- Substantial public interest
- Health and social care purposes
- Legal claims and judicial acts

Safeguarding Processing: Much of our data processing for safeguarding purposes relies on legal obligation and vital interests bases, as outlined in our **Child Protection Procedures** and **Adult Safeguarding Procedures**.

6. Consent Management

Consent is one of our key lawful bases for processing personal data. BYO ensures all consent meets GDPR standards and is properly managed throughout the data lifecycle.

Consent Requirements

Valid consent must be:

- **Freely given** - Individuals have genuine choice and control
- **Specific** - Clearly covers the particular processing activity
- **Informed** - Individuals understand what they're consenting to
- **Unambiguous** - Clear positive action required (no pre-ticked boxes)
- **Granular** - Separate consent for different processing purposes
- **Easily withdrawable** - Simple process to withdraw consent at any time

Photography and Videography Consent

Consent for photography and videography is obtained during our registration process through a clear, specific consent mechanism. This consent covers:

- Social media promotion and marketing materials
- Website content and promotional materials
- Fundraising and grant application documentation
- Media engagement and press materials
- Internal documentation and training purposes

Children's Consent

For children under 13:

- We obtain parental/guardian consent for all processing based on consent
- We assess whether the child is competent to understand and consent independently
- We consider safeguarding implications when parents/guardians exercise children's rights
- We balance children's developing autonomy with protection requirements

For children aged 13-16, we assess competence on a case-by-case basis, considering the nature of processing and potential risks.

Safeguarding Considerations: When parental involvement may put a child at risk, we follow procedures outlined in our **Child Protection Procedures** and consult with our **DSL**.

Consent Withdrawal

Individuals can withdraw consent by:

- Contacting the Data Protection Lead directly
- Using unsubscribe links in communications
- Requesting withdrawal through any staff member
- Submitting written requests

We action all consent withdrawals within 48 hours and confirm the change in writing.

7. Responsibilities

Board of Directors

- Ultimate accountability for data protection compliance
- Ensuring adequate resources for data protection activities
- Oversight of data protection risk management

Designated Safeguarding Lead (DSL)

Joshua William Hall

- Mobile: 07597 874 222
- Email: joshuahall@britanniayo.com

Responsibilities:

- Ensuring safeguarding data processing compliance
- Authorising information sharing for safeguarding purposes
- Liaison with Data Protection Lead on safeguarding data matters

Data Protection Lead (Project Manager)

[To be designated]

- Day-to-day operational responsibility for data protection compliance
- Staff and volunteer training coordination
- Handling subject access requests and data protection queries
- Managing relationships with data processors
- Investigating and reporting data breaches
- Maintaining data protection documentation

All Staff, Directors and Volunteers

- Processing personal data only in accordance with this policy
- Completing required data protection training
- Reporting potential data breaches immediately
- Respecting individuals' rights regarding their personal data
- Following security procedures for handling personal data

Training Requirements: Data protection training is integrated with safeguarding training as outlined in our **Safeguarding Policy Framework**.

8. Data Security

BYO implements appropriate technical and organisational measures to protect personal data, including:

Technical Measures

- Secure storage systems with access controls
- Regular security updates and patches
- Encryption for sensitive data transmission
- Regular backups with secure storage
- Password protection and multi-factor authentication
- Secure disposal of electronic data

Organisational Measures

- Staff training on information security
- Clear desk and screen policies
- Secure disposal of confidential waste
- Access controls and authorisation procedures
- Incident response procedures
- Regular security reviews and audits

Digital Safety: Our approach to online data security aligns with our **Digital Safeguarding Policy**.

9. Safeguarding and Information Sharing

Safeguarding Data Processing

BYO processes personal data for safeguarding purposes under the lawful bases of:

- **Legal obligation** - Statutory duties to protect children and adults at risk
- **Vital interests** - Protection of life and safety
- **Substantial public interest** - Safeguarding children and adults

Information Sharing for Safeguarding

We may share personal data without consent when:

- Required by law (e.g., reporting to local authority)
- Necessary to protect a child or adult at risk
- Needed to prevent or detect crime
- Required for legal proceedings

See Also: Detailed information sharing procedures are outlined in our **Child Protection Procedures** and **Adult Safeguarding Procedures**.

Balancing Confidentiality and Protection

When sharing information for safeguarding:

- We consider the data protection impact
- We share only necessary information
- We document the decision-making process
- We inform individuals where safe and appropriate to do so

Professional Guidance: Our DSL provides guidance on balancing data protection with safeguarding requirements.

10. Data Sharing and Third Parties

We only share personal data where we have a lawful basis and appropriate safeguards in place. Data may be shared with:

Statutory Sharing

- **Local Authority Safeguarding Teams** - Legal obligation
- **Police** - Crime prevention and detection
- **Health Services** - Child protection and welfare
- **Courts** - Legal proceedings

Operational Sharing

- **Funding bodies** - Grant reporting (legitimate interest)
- **Professional advisors** - Legal or administrative purposes (legitimate interest)
- **Emergency services** - Crisis situations (vital interests)
- **Partner organisations** - Service delivery (legitimate interest with appropriate agreements)

Complaints Route: If individuals are concerned about our information sharing, they can use our **Complaints Policy** procedures.

11. Data Retention and Disposal

We retain personal data only for as long as necessary to fulfil our stated purposes. Our retention schedule covers:

Retention Periods

- **Participant records** - 25 years after last contact (safeguarding considerations)
- **Safeguarding records** - Permanently with secure storage arrangements
- **Staff and volunteer records** - 6 years after leaving (50 years for pension information)
- **Financial records** - 7 years as required by HMRC
- **General administration** - 3 years unless specific legal requirements apply
- **Complaints records** - 6 years after resolution
- **Photography/video content** - Until consent withdrawn or 25 years

Secure Disposal

Data is securely destroyed when retention periods expire, using:

- Professional shredding for paper records
- Secure data wiping for electronic devices
- Certificate of destruction for sensitive materials
- Witnessed destruction for highest sensitivity items

Safeguarding Records: Safeguarding records are retained permanently due to the potential for historic abuse disclosure, as outlined in our **Child Protection Procedures**.

12. Individual Rights

All individuals have the right to:

- **Be informed** about how their data is used (transparency)
- **Access** their personal data (subject access requests)
- **Rectification** of inaccurate or incomplete data
- **Erasure** in certain circumstances ('right to be forgotten')
- **Restrict processing** in specific situations
- **Data portability** where technically feasible
- Object to processing based on legitimate interests or direct marketing
- **Avoid automated decision-making** including profiling
- **Complain** to the Information Commissioner's Office
- **Seek compensation** for damages caused by data protection breaches

Limitations for Safeguarding

Some rights may be limited where exercising them would:

- Prejudice safeguarding investigations
- Put a child or adult at risk
- Interfere with legal proceedings
- Compromise crime prevention

The DSL advises on such limitations in consultation with the Data Protection Lead.

Subject Access Requests

We respond to subject access requests within one month, providing:

- Confirmation of processing
- Purposes of processing
- Categories of data held
- Recipients of data
- Retention periods
- Rights available

Complex Requests: Requests involving safeguarding records require consultation with our DSL and may involve redaction to protect third parties.

13. Data Breaches

A data breach is any security incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Breach Response Procedure

1. **Immediate containment** - Stop the breach and assess the situation
2. **Risk assessment** - Evaluate potential harm to affected individuals
3. **Notification to DSL** - If safeguarding data involved
4. **Documentation** - Record all relevant details of the incident
5. **ICO notification** - Within 72 hours if high risk
6. **Individual notification** - If high risk to their rights
7. **Investigation** - Determine root cause and prevent recurrence
8. **Review** - Update procedures based on lessons learned

Safeguarding Data Breaches

Breaches involving safeguarding data require:

- Immediate notification to DSL
- Assessment of risk to vulnerable individuals
- Consideration of notification to statutory agencies
- Enhanced monitoring and support

Reporting Route: Staff unsure about breach reporting can use our **Whistleblowing Policy** for guidance.

14. Digital Platforms and Online Safety

Social Media and Digital Platforms

Our use of digital platforms is governed by:

- **Social Media Policy** - Platform-specific guidance
- **Digital Safeguarding Policy** - Online safety measures
- **Photography and Videography Policy** - Image sharing protocols

Online Data Processing

When using online platforms, we:

- Conduct privacy impact assessments
- Review platform privacy policies
- Implement appropriate privacy settings
- Monitor for unauthorised data sharing
- Provide training on safe platform use

See Also: Comprehensive online safety guidance is provided in our **Digital Safeguarding Policy**.

15. Complaints and Concerns

Internal Complaints

Individuals can raise data protection concerns by:

- Contacting the Data Protection Lead directly
- Using our Complaints Policy procedures
- Speaking to any member of staff who will escalate appropriately

We investigate all complaints promptly and provide written responses within one month.

External Complaints

If unsatisfied with our response, individuals can:

- **Information Commissioner's Office**: ico.org.uk or 0303 123 1113
- **Citizens Advice** for independent guidance
- **Legal advice** where appropriate

Whistleblowing: Staff with concerns about data protection compliance can use our **Whistleblowing Policy** for protected reporting.

16. Training and Compliance

Training Programme

All individuals with access to personal data receive training on:

- Data protection principles and requirements
- Individual responsibilities and accountability
- Recognising and reporting data breaches
- Secure handling and storage of personal data
- Respecting data subjects' rights
- Safeguarding and information sharing

Compliance Monitoring

We maintain comprehensive records including:

- Data processing activities register
- Data sharing agreements
- Training records
- Subject access request logs
- Data breach incident reports
- Privacy impact assessments
- Consent records and withdrawals

17. Related Policies

This policy should be read alongside:

- **Safeguarding Policy Framework**
- **Child Protection Procedures**
- **Adult Safeguarding Procedures**
- **Photography and Videography Policy**
- **Social Media Policy**
- **Digital Safeguarding Policy**
- **Complaints Policy**
- **Whistleblowing Policy**
- **Code of Conduct Policy**
- **Anti-Bullying Policy**
- **Health and Safety Policy**

Policy Review and Updates

This policy is reviewed every two years by the Data Protection Lead and DSL, with Board approval required for significant changes. Emergency updates may be made to address legislative changes or significant incidents.

Next scheduled review: 17/06/27

Document Control:

- This policy forms part of BYO's information governance framework
- All staff receive mandatory training on data protection requirements
- Regular audits ensure ongoing compliance with legal requirements

Reviewed by:

Hassan Kingsley, Governor
Date: 18/06/2025
Next Review Date: 18/06/2027

This policy forms part of BYO's commitment to safeguarding and should be read alongside our complete Safeguarding Framework.

Britannia Youth Organisation CIC is a Community Interest Company registered in England and Wales. Company No. 12515346 | Registered Address: 36 St Joseph's Rd, Ward End, Birmingham, B8 2JU