UK YOUTH

Data Protection and Privacy Policy

Contents

Data Protection and Privacy Policy

Purpose

This policy outlines how UK Youth ensure secure, lawful, and accountable processing, storage, transfer, and retention of personal and sensitive data through its ICT systems. It applies data protection principles to the full data lifecycle, integrating requirements around privacy, confidentiality, data minimisation, and data subject rights. The policy supports compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It includes governance tools such as Data Protection Impact Assessments (DPIAs), privacy notices, retention protocols, and international data security controls. It ensures that digital systems, cloud services, and remote working environments are managed to protect individuals' data and the organisation's integrity.

Scope

This policy applies to all staff, volunteers, contractors, and partners using, managing, or accessing UK Youth's ICT systems that store, process, or transfer personal or sensitive data. It covers all data processing activities conducted using UK Youth-provided hardware, software, platforms (including cloud-based systems), and accounts, whether on-site, remotely, or during international travel. This includes activities involving mobile devices, collaboration tools, digital platforms, or any scenario where data may be shared, accessed, or stored using UK Youth systems or credentials or any scenario where data may be shared, accessed, or stored using UK Youth systems, credentials, or automated technologies such as AI-powered tools.

Roles and Responsibilities

Clear roles and responsibilities are essential for ensuring consistent compliance with data protection obligations. The table below outlines the key responsibilities for individuals and teams handling personal and sensitive data within UK Youth's ICT systems.

Operational Roles and Responsibilities

Role	Responsibilities
All Staff, Volunteers, Contractors	• Complete mandatory annual data protection training • Use approved systems and follow secure data handling guidance (incl. during travel) • Immediately report breaches or suspected risks to the DPO
Line Managers	• Ensure team members understand and follow this policy

Role	Responsibilities
	• Support DPIAs and implementation of controls • Oversee leaver handovers and access revocation
ICT Team	• Maintain secure digital infrastructure (encryption, MFA, backups) • Support labelling, retention, and deletion protocols • Assist in breach containment and forensic review
Operations Team	• Approve international travel involving UK Youth devices • Provide travel-related security briefings • Act as first contact for ICT issues arising during travel

Governance and Oversight Roles

Role	Responsibilities
Data Protection Officer (DPO)	• Lead on UK GDPR and DPA 2018 compliance • Review and approve DPIAs • Advise on legal bases, privacy notices, individual rights, and data sharing • Report notifiable breaches to the ICO • Maintain Breach Log and provide quarterly oversight reports • Advise on AI-specific compliance obligations, including transparency, human review, and risk mitigation requirements • Ensure AI-related decisions and profiling tools meet fairness, explainability, and legal standards
Chief Executive Officer (CEO)	• Hold overall accountability for data protection and governance • Promote a culture of data protection by design across functions
Trustees	• Provide strategic oversight and ensure compliance through board reporting mechanisms
Legal Support	• Review DSAs, DPAs, and agreements involving complex data use, international transfers, or unfamiliar jurisdictions • Support interpretation of UK GDPR, PECR, and other legal obligations

📌 All DPO consultations should be recorded in the central UKY Data Log on the UKY Personal Data sheet located on SharePoint at: K:\Operations\Data\UKY Personal Data Log.

Policy Statements

Definitions

To support consistent understanding and application of this policy, the following key terms are defined in line with the UK GDPR and Data Protection Act 2018:

Term	Definition
Personal Data	Any information that relates to an identified or identifiable individual (data subject), such as a name, email address, identification number, or location data.
Special Category Data	A subset of personal data that is more sensitive and requires greater protection. It includes data about racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, and biometric or genetic data.
Data Subject	The individual to whom the personal data relates.
Data Controller	The organisation or person that determines the purposes and means of processing personal data. UK Youth is a data controller for most of its activities.
Data Processor	A third party that processes personal data on behalf of the data controller under a written contract.
Processing	Any action performed on personal data, including collection, storage, use, sharing, or deletion.
Data Protection Impact Assessment (DPIA)	A risk assessment process is required for processing activities likely to result in a high risk to individuals' rights and freedoms.
Data Breach	A security incident in which personal data is lost, accessed without authorisation, altered, disclosed, or destroyed.

Term	Definition
Encryption	A security measure that protects data by converting it into a coded format that can only be read with a decryption key.
UK GDPR	The United Kingdom General Data Protection Regulation is the UK's primary legal framework for personal data protection post-Brexit.

Data Protection Principles

All data processing must comply with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

To understand our Data Protection Requirements, see **Appendix 1**.

The use of Artificial Intelligence to process personal data will strictly adhere to the UK Youth Use of AI policy.

Privacy and Confidentiality

- Data must only be accessed by authorised individuals based on job responsibilities.
- Confidential information must be handled with discretion and transmitted through secure, approved ICT systems.
- All users must complete mandatory data protection training annually.
- All personal and sensitive data must be treated as confidential and accessed only by individuals with an explicit and lawful need to know.
- Staff, volunteers, contractors, and partners must not disclose personal data to unauthorised individuals or use it for purposes beyond those approved.
- Breaches of confidentiality, whether intentional or accidental, will be treated as data protection breaches and may result in disciplinary action or legal consequences.

To understand our Privacy and Confidentiality Requirements, see **Appendix 2**.

Data Retention

- Personal data must only be retained for as long as relevant for the purpose(s) for which the data was initially collected.
- Retention periods vary based on data category and legal requirement.
- Secure disposal (deletion or anonymisation) must be performed once retention periods expire.

To understand our Record Retention Requirements, see **Appendix 3**.

Privacy Notices

- Privacy notices must be provided at the point of data collection and must include:
    - Purpose of collection
    - Legal basis for processing
    - Data recipients
    - Retention periods
    - Data subject rights

Please refer to **Appendix 4** for our Privacy Notice Guidelines.

📌 The *Privacy Notices for the Published (website), Employment*, *Recruitment*, and *Children & Young People* are available in the Policy Hub on SharePoint.

Supporter Profiling and Wealth Research

As part of its fundraising strategy, UK Youth may, where permitted by law, conduct wealth screening and supporter profiling to identify individuals interested in providing substantial philanthropic support. This processing helps ensure that fundraising communications and engagement efforts are efficient, proportionate, and aligned with individual interests.

We may conduct in-house research or engage specialist third parties (e.g., Prospecting for Gold, Factary) under data processing agreements. Information used in profiling may include:

- Existing data from our relationship with the supporter
- Public records (e.g., Companies House, Charity Commission)
- Reputable media sources, rich lists, or biographical databases
- Public social media profiles or websites

This processing is based on legitimate interest and must be supported by a legitimate interest assessment (LIA) and, where appropriate, a Data Protection Impact Assessment (DPIA).

Supporters must be informed of this practice through our published Privacy Notice and allowed to opt out.

All data used in profiling must be accurate, relevant, and collected following data minimisation principles. Individuals' rights under the UK GDPR—such as the right to object to processing for profiling purposes—must always be upheld.

Where AI tools are used, they must offer enterprise-grade privacy assurances (e.g. no data retention, no training on user inputs).

Data Protection Impact Assessments (DPIAs)

- DPIAs must be completed for any ICT project or initiative involving high-risk personal data processing (e.g., large-scale data use, new systems).
- DPIAs must be started early in the project lifecycle, approved by the DPO, and stored securely.

Projects involving **a**utomated decision-making, AI tools, machine learning, algorithmic profiling, or new technologies that could affect individuals' rights must be subject to a DPIA and reviewed by the DPO and Legal Support, as appropriate.

This includes tools that:

- Make decisions about individuals without human involvement
- Analyse behaviour for profiling or targeting
- Use biometric data or facial recognition

Projects must demonstrate data protection by design and ensure lawful, fair, and transparent use of emerging technologies where relevant.

Please refer to our DPIA Guidelines (**Appendix 5**) for support in consistently completing this task.

📌 Our *Data Protection Impact Assessment (DPIA) Template* is available in the Policy Hub on SharePoint.

International Data Security and Travel Requirements

To safeguard organisational and personal data when travelling internationally, staff, volunteers, and contractors must follow the measures below when handling UK Youth ICT equipment or data abroad.

a. Pre-Travel Requirements

- Staff travelling internationally with UK Youth ICT equipment must consult the NCSC Secure Travel Abroad Guidance and FCDO Travel Advice to assess data security risks and determine if a destination is considered high-risk.

- Notify the ICT Team and the Head of Operations *before* planning any international travel involving UK Youth devices. **Approval is required, especially for high-risk countries.**
- Backup and sanitise devices: Remove non-essential files and sensitive content before travel; store working files on UK Youth's secure cloud storage (e.g., OneDrive).
- Update and encrypt devices: Ensure all software is up to date and device encryption is enabled. Some countries may prohibit the use of encrypted devices, so please check local regulations.
- Use strong authentication: Enable multi-factor authentication (MFA) on all accounts. Change passwords before departure using a secure method.
- Travel light: Bring only essential devices and data. Use "clean" devices that can be wiped after travel.

b. Device and Data Use During Travel

- Avoid public Wi-Fi and terminals: Never access UK Youth cloud services or confidential data using unsecured networks or public machines.
- Limit connectivity: Disable Wi-Fi and Bluetooth when not in use, and power off devices at borders or checkpoints.
- Browser hygiene: Use private browsing modes, and clear history, cache, and cookies after each use.
- Be alert: Monitor for suspicious device activity or prompts. Do not plug in untrusted USB devices.

c. Post-Travel Security Actions

- Run antivirus scans on all devices used during travel.
- Change passwords again upon return.
- Report issues immediately: If you suspect a data breach, device loss, or malware infection, notify the ICT Team and the DPO promptly.

d. High-Risk Destinations or Travellers

- If you travel to a high-risk region or carry sensitive data, contact the ICT Team and Head of Operations for tailored risk assessment and security advice.

Cookie Use

UK Youth's websites use cookies to support functionality, understand user engagement, and improve services. Cookies are small text files stored on your device when you visit a website. We use:

- **Essential cookies** – These are required for the website to function correctly (e.g., for navigation and security).
- **Analytics cookies** – Help us understand how visitors use our site (e.g., pages visited, time spent).
- **Preference cookies** – Remember your choices (e.g., language settings).

We do **not** use cookies for advertising or third-party tracking.

You can manage or turn off cookies through your browser settings at any time. However, turning off essential cookies may affect site functionality.

Use of Artificial Intelligence

UK Youth acknowledges the legal, ethical, and operational responsibilities associated with the use of Artificial Intelligence (AI) and automated decision-making tools. All such applications must be transparent, explainable, and subject to appropriate human oversight where decisions could have legal or significant effects on individuals.

The organisation is committed to upholding individuals' rights to understand, contest, and request human review of decisions made solely through AI systems.

All AI tools used to generate or process content must comply with UK Youth's AI Usage Policy. Public or free versions of AI tools must not be used to process sensitive, confidential, or personal data.

AI-generated content must not be discriminatory, misleading, or manipulative, and must be subject to human review before use in decision-making, particularly where vulnerable groups are involved.

Where staff propose new uses of AI, a business case must be submitted to the DPO and relevant Director prior to deployment, in line with the AI Usage Policy.

Data Sharing and Third-Party Processing

UK Youth is committed to ensuring that any sharing of personal data is lawful, transparent, and in line with data protection principles.

Data Sharing Agreements (DSAs)

When UK Youth share personal data with another organisation acting as a separate data controller (e.g. a partner charity or funder), a Data Sharing Agreement must be in place. The agreement must set out:

- The purpose and legal basis for sharing
- Roles and responsibilities of each party

- Data types and retention periods
- Safeguards to protect the data

Data sharing must be proportionate, documented, and approved by the relevant manager or the Data Protection Officer (DPO).

📌 Our *Data Sharing Agreement (DSA) Template* is available in the Policy Hub on SharePoint.

Third-Party Processors (Data Processing Agreements)

Where UK Youth engages a third party to process personal data on its behalf (e.g., cloud services, IT providers, survey platforms), the third party is considered a data processor under the UK GDPR.

In such cases, a **Data Processing Agreement (DPA)** must be in place and must:

- Clearly define the processor's duties
- Require compliance with UK GDPR Article 28
- Include security, breach notification, and confidentiality clauses
- Prohibit further sub-processing without written consent

All processors must undergo due diligence and be documented in the Processor Register, which the Operations Team maintains.

📌 Our *Data Processing Agreement (DPA) Template* and *Processor Register* are available in the Policy Hub on SharePoint.

Approval Process for a DSA and DPA

1. Relevant Operational Lead / Manager
   - Reviews the purpose and necessity of the data sharing
   - Confirms alignment with programme, partnership, or contractual needs

2. Data Protection Officer (DPO)
   - Verifies the legal basis under UK GDPR
   - Ensures the DSA includes all required clauses (e.g. rights, retention, breach notification)
   - Confirms data minimisation, proportionality, and risk controls

3. Director of Operations (or equivalent)
   - Signs off on agreements involving **moderate or high-risk data** (e.g. young people, safeguarding, special category data)

- May delegate lower-risk agreements (e.g. contact info for logistics) to managers

Legal review may be required if the agreement involves:

- International transfers
- Complex data use (e.g. AI, profiling)
- Unfamiliar jurisdictions
- Sensitive partner negotiations
- New types of data partnerships

Before data is shared, *each party (UK Youth and the external controller) must sign the agreement, including their names and titles.*

Oversight and Breach Response

Where personal data is shared externally or processed by a third party:

- The relevant contract or agreement must include clauses about breach notification timelines and responsibilities.
- The DPO must be informed immediately of any suspected or confirmed breach involving external parties.
- All DSA and DPAs must be recorded in the organisation's Live Processor Record, including details of the incident, its impact, and any remedial actions taken.

For support in reviewing agreements or assessing a proposed processor, contact data@ukyouth.org.

📌 The UK Youth Data Log, including the Live Processor Record sheet, is maintained by the Data Protection Officer and stored in a secure, access-controlled location on the organisation's Microsoft 365 platform. Access is restricted to authorised personnel. *This is the official location for documenting all personal data breaches, regardless of severity.*

Personal Data Breach Management

Any staff member, volunteer, or contractor must **immediately report** all suspected or confirmed personal data breaches to the DPO.

A data breach may include (but is not limited to):

- Loss or theft of devices or documents
- Unauthorised access to personal data
- Accidental disclosure or sending of data to the wrong recipient
- Malware or phishing attacks that compromise information

Reporting Process

- Notify the DPO at data@ukyouth.org as soon as the breach is discovered.
- Complete a breach report using the organisation's Data Incident Reporting Form, available in the Policy Hub on SharePoint.
- If the breach occurs during travel, notify the Operations Team and follow international security protocol.

Containment and Assessment

- The DPO will coordinate an immediate risk assessment to:
    - Identify the nature and scope of the breach
    - Contain the breach and mitigate further loss
    - Assess the impact on individuals and the organisation

Notification

- If the breach risks individuals' rights and freedoms, the DPO will notify the Information Commissioner's Office (ICO) within **72 hours** of becoming aware of the breach.
- Where appropriate, affected individuals will also be informed without undue delay and given clear guidance on protecting themselves.

Breach Response Procedure and Record-keeping

- UK Youth's Personal Data Breach Response Procedure outlines detailed steps for investigation, containment, notification, and post-incident review.
- All breaches, regardless of severity, must be documented in the organisation's Personal Data Breach Reporting Log, including details of the incident, its impact, and any remedial actions taken.

📌 The UK Youth Data Log, including the Breach Reporting Log sheet, is maintained by the Data Protection Officer and stored in a secure, access-controlled location on the organisation's Microsoft 365 platform. Access is restricted to authorised personnel. *This is the official location for documenting all personal data breaches, regardless of severity.*

Review and Amendment

The DPO will formally review this policy annually, in consultation with the Operations, ICT, and People teams. Reviews may also take place earlier in response to:

- Significant legal or regulatory changes (e.g. amendments to the UK GDPR or DPA 2018)
- Organisational changes that impact data processing (e.g. system migrations, international expansion)
- Lessons learned from data protection incidents or audits
- Anticipated legal developments in the UK or EU regarding the regulation of Artificial Intelligence and algorithmic decision-making.

All material amendments to this policy must be approved by the relevant governance body (e.g. the Board or an appropriate subcommittee). Once approved, changes will be communicated to all staff, volunteers, and contractors. Where relevant, updated training, briefings, or guidance will be provided to ensure ongoing compliance and understanding.

All superseded versions will be archived, and version history will be maintained.

Related Policies

- Digital and Acceptable Use Policy (DAUP)
- BYOD Guidelines (Supplement to DAUP)
- Information Security and Breach Response Policy
- Remote Working, Mobile Device, and Mobile Phone Eligibility Policy
- Safeguarding Policy
- Digital Safeguarding Policy
- Data Classification and Handling Policy
- ICT Encryption Policy

Appendices

Appendix 1 – Data Protection Requirements
Appendix 2 – Privacy and Confidentiality Requirements
Appendix 3 – Record Retention Requirements
Appendix 4 – Privacy Notice Guidelines
Appendix 5 – DPIA Guidelines

Document Control

Document Name:	ICT Data Protection and Privacy
Issue Number:	01
Document Owner:	Director, Finance & Operations, with review by Data Protection Officer
Document Manager:	ICT Manager, Head of Operations
Date:	August 2025
Review Date:	August 2026
Related Laws and Regulations:	1. UK General Data Protection Regulation (UK GDPR) 2. Data Protection Act 2018

3. Privacy and Electronic Communications Regulations (PECR) 2003
4. UK GDPR Part 3 & International Transfers Provisions
5. Local Data Laws in countries visited during international travel
6. Computer Misuse Act 1990
7. National Cyber Security Centre (NCSC) Guidance and Cyber Essentials Framework
8. Charity Commission Requirements (including CC8 guidance)
9. Employment Rights Act 1996 and related employment legislation

Document History:

V01: Consolidated and replaces the original UK Youth Policies & Procedures:

- Data Protection Requirement (3.1)
- Retention of Records Requirement (3.3, Retention Labels V3)
- Confidentiality (3.5)
- Privacy and Notices (3.4, 3.7, 3.8, 3.9)
- DPIA Template and Guidance (12.5, 12.5.1, 3.6)

The document was approved by:

PROVISIONAL, pending approval by Finance, Risk and Audit Committee

This Level 2 essential organisational policy requires approval by board committee.

Appendix 1

Data Protection Requirements

UK Youth complies fully with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All staff, volunteers, contractors, and partners using ICT systems must adhere to the following data protection requirements:

1. Lawful Processing

- Personal data must be processed lawfully, fairly, and transparently.
- A valid legal basis must be documented for each processing activity.

2. Purpose Limitation

- Data may only be used for the purpose specified at the time of collection.
- Any new or significantly different use must be reviewed, and where required, supported by a DPIA and updated privacy notice.

3. Data Minimisation and Accuracy

- Only data that is adequate, relevant, and necessary should be collected.
- Personal data must be kept accurate and up to date.

4. Storage Limitation

- Data must only be retained for as long as necessary following the Retention Schedule.
- Secure disposal or anonymisation is required once retention ends.

5. Security and Integrity

- Data must be protected against unauthorised access, loss, or damage.
- UK Youth systems must use encryption, access controls, backups, and strong passwords.

6. Rights of Data Subjects

Individuals (data subjects) have the right to:

- Be informed via clear privacy notices
- Access their data (subject access request)
- Request rectification of inaccurate data
- Request erasure of data ("right to be forgotten")
- Restrict processing (e.g. while accuracy or lawfulness is being verified)
- Data portability (to receive and reuse their data)
- Object to processing (e.g. for direct marketing or under legitimate interest)
- Challenge decisions made solely through automated processing, including AI or profiling, and request human intervention, explanation, and reconsideration of such decisions

7. Data Sharing and Transfers

- Personal data may only be shared externally with appropriate safeguards (e.g. DPAs, DSAs).
- International transfers (outside the UK/EEA) require legal safeguards and DPO approval.

8. Data Breaches

- All actual or suspected personal data breaches must be reported to the DPO immediately.
- The DPO will assess risk and, if necessary, report to the ICO within 72 hours.

9. Training and Responsibilities

- All staff must complete annual data protection training.
- Managers must monitor compliance within their teams.
- Trustees and the CEO hold ultimate accountability for governance.

Appendix 2

Privacy and Confidentiality Requirements

UK Youth is committed to protecting personal data and ensuring transparency when collecting, using, and sharing it through digital and ICT systems. These requirements apply to all data collected or processed online (e.g. websites, email, cloud platforms, booking systems).

a. Transparency and Lawful Basis

- Individuals must be informed at the point of collection about:
  - The purpose of processing
  - The lawful basis (e.g. consent, contract, legal obligation, legitimate interest)
  - Data sharing and international transfers
  - Retention periods
  - Their data protection rights
  - Where applicable, details of any automated decision-making or profiling using AI, including how decisions are made, their significance, and the individual's right to request human review
- Privacy notices must be clear, accessible, and appropriate for the audience (e.g. children, employees, supporters).

b. Consent and Legitimate Interest

- Consent must be explicit, informed, and easy to withdraw.
- Legitimate interest processing must be supported by a balancing test and respect individuals' rights.

c. Data Sharing and Trusted Partners

- Data may only be shared externally when:
  - It is essential for delivering services, and
  - A Data Sharing or Processing Agreement is in place
- Data must never be sold or shared with direct marketing companies without explicit consent.

d. Children and Young People

- Where services are accessible to those under 16:
  - Systems must clearly explain data use
  - Parental consent should be obtained where required
- Marketing communications must not be knowingly sent to children under 16.

e. Security of Information

- All personal data must be stored using secure, encrypted systems with access controls.
- International transfers require legal safeguards (e.g. SCCs or adequacy decisions).
- Only individuals with a lawful and clearly defined need may access personal or sensitive data.
- Unauthorised disclosure or use of personal data is prohibited.

f. Cookies and Analytics

- Users must be notified of cookie use and given options to manage preferences.
- Analytics tools must not identify individuals without valid consent.

g. Individual Rights

Individuals have the right to:

- Access their data
- Request correction or erasure
- Withdraw consent
- Object to processing
- Request data portability
- Restrict processing (e.g. when accuracy or lawfulness is in question)
- Challenge decisions made solely through automated processing, including AI and profiling
    - This includes the right to request human intervention, express their view, and contest outcomes
- Lodge complaints with the Information Commissioner's Office (ICO)

h. Changes and Further Processing

- If data will be used for a new purpose, updated privacy notices and (where required) renewed consent must be obtained.
- Significant changes to privacy practices must be communicated clearly and made publicly accessible.

Appendix 3

Record Retention Requirements

UK Youth retains personal data only for as long as necessary for operational, legal, and regulatory purposes. These requirements apply to all physical and digital records held within ICT systems or associated with them.

a. General Principles

- Records must not be retained longer than necessary.
- Retention decisions must reflect legal, contractual, and business needs.
- Personal data must be disposed of securely once the retention periods expire.
- All record retention practices must comply with the UK GDPR, the Data Protection Act 2018, and relevant sector-specific laws.

b. Statutory Retention Requirements

To ensure compliance, UK Youth follows a combination of:

1. **Legal/statutory requirements** (e.g. HMRC, Companies Act, employment law),
2. **Regulatory guidance** (e.g. Charity Commission, ICO, Fundraising Regulator),
3. **Best practice recommendations** (e.g. NCVO, CIPFA, sector-specific bodies).

While the standard retention period for UK Youth records/information is 6 years, we are mindful that core categories and common retention periods relevant to UK charities can vary. UK Youth utilises these resources to assess Data Retention best practices:

- **ICO**: Data Protection and Retention
- **Charity Commission**: Operational guidance and trustee duties
- **HMRC**: Guidance on financial and tax recordkeeping
- **ACAS**: Employment and HR records
- **NCVO / CIPFA**: Sector best practice
- **Fundraising Regulator**: Retention for donor and marketing data

Data Type	Recommended Retention Period	Statutory Basis/Guidance
Financial records	6 years	Companies Act 2006, Charities Act 2011, HMRC
Gift Aid declarations	6 years after the last donation	HMRC
Employee records	6 years after employment ends	Limitation Act 1980
Payroll & PAYE records	3 years	HMRC
Accident books/health and safety records	3 years (adults) / Until the child turns 21	RIDDOR 2013
Contracts	6 years after expiry	Limitation Act 1980
Pension records	6 years or longer (some up to 12 years)	The Pensions Regulator
Volunteer records	3–6 years after involvement ends	Best practice (NCVO)

Data Type	Recommended Retention Period	Statutory Basis/Guidance
Safeguarding records	75 years or more	NSPCC, Charity Commission best practice
Board minutes / governing documents	Permanently	Charity Commission
Donor records	6 years after the last contact	Fundraising Regulator, GDPR (legitimate interest basis)
Marketing consent (GDPR)	Until withdrawn or reconsent obtained (review every 2 years)	ICO
Insurance records (including claims)	40 years	Best practice, insurance industry norms
Disciplinary / grievance records	6 years after the case is closed	ACAS, Limitation Act

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained when essential for a business to operate effectively. Under GDPR and the DPA 2018, personal data processed by UK Youth must not be retained for longer than is necessary for its lawful purpose.

Records/information must only be retained beyond the default retention period if justified by statutory, regulatory, legal, or security reasons or their historical value.

Before disposing of high-risk data categories, such as safeguarding records, financial data, or donor information, approval must be obtained from the relevant senior manager or data owner to ensure legal, reputational, or operational risks have been assessed.

c. Non-Statutory Retention (Best Practice)

For records without a legal mandate, UK Youth follows recommended periods based on risk and the Limitation Act 1980:

- **Personnel files** – 6 years after employment ends
- **Parental leave records** – 5 years (or 18 years if the child receives disability allowance)
- **Recruitment records (unsuccessful candidates)** – 1 year

d. Secure Disposal Requirements

- **Paper records** must be shredded, pulped, or incinerated.
- **Digital data** must be deleted from systems and email bins, and irretrievably removed from media.
- **IT equipment** and **removable media** must be physically destroyed or wiped using certified tools.
- **Third-party disposal** must be under contract with confidentiality and data protection clauses.

e. Online Systems and Microsoft 365

- Deleted items remain in Microsoft bins for 30 days and are not "beyond use" until emptied.
- Leavers' accounts must be reviewed, and necessary handovers must be completed before deactivation.

Appendix 4

Privacy Notice Guidelines

UK Youth is committed to ensuring transparency and compliance with the law when collecting and processing personal data. Privacy notices are the primary tool for informing individuals about how their data will be used. They are essential for demonstrating compliance with the UK GDPR and the Data Protection Act 2018.

a. Purpose of Privacy Notices

Privacy notices explain:

- What personal data is collected
- The purpose and legal basis for processing
- How the data will be used, shared, and stored
- How long will the data be retained
- The rights of the data subject, including:
  - ✓ The right to access, correct, or erase data
  - ✓ The right to object to processing
  - ✓ The right to restrict processing
  - ✓ The right to object to and seek human review of decisions made solely by automated means, including those involving Artificial Intelligence (AI) or profiling
- Contact details for further information or complaints

b. When to Use a Privacy Notice

A privacy notice must be provided:

- At the point of data collection (whether digital or physical)
- When data is collected from a third party (as soon as reasonably possible)
- In any project involving personal data processing, including recruitment, employment, programme delivery, and youth engagement

c. Types of Privacy Notices

UK Youth maintains and regularly reviews tailored privacy notices, including:

- Recruitment Privacy Notice – Outlines the personal data collected from job applicants and how it is used to assess suitability for employment, including any automated decision-making involved in shortlisting or screening processes.
- Employment Privacy Notice – Describes how staff data is processed throughout the employment lifecycle, including systems used for performance management, HR analytics, or compliance monitoring.
- Children & Young People Privacy Notice – Written in a simplified, age-appropriate format to ensure understanding and parental consent where applicable, particularly where data may be used in digital platforms or systems involving behavioural tracking or profiling.

- **Published Privacy Notice (Website)** – Provides a general overview of data collection via UK Youth's online platforms and includes clear information about cookies, analytics, and any use of AI or profiling tools, along with the right to object to automated decision-making and request human review.

d. Content Guidelines

Each privacy notice must include:

- Contact details for the Data Protection Officer (DPO)
- Types of personal data being collected, including any special category or sensitive data
- With whom the data may be shared, including third parties or processors
- Whether data will be transferred outside the UK/EEA, and the safeguards in place for such transfers
- The lawful basis for processing (e.g. consent, contract, legal obligation, legitimate interest)
- The individual's rights under data protection law, including:
  - ✓ The right to access, rectify, or erase data
  - ✓ The right to object to or restrict processing
  - ✓ The right to object to automated decision-making, including profiling, and to request meaningful human involvement in decisions that significantly affect them
- How long the data will be retained, and how it will be securely disposed of when no longer needed
- Details of any automated decision-making or AI technologies used, including:
  - ✓ The logic involved in the processing
  - ✓ The potential impact or consequences for the individual
  - ✓ How individuals can exercise their rights concerning such processing

e. Consent and Age-Appropriate Language

- For individuals under 16, consent must be obtained from a parent or guardian.
- Notices aimed at children must be written in clear, understandable language.

f. Accessibility and Format

- Notices should be published on the organisation's website and available in printed format upon request.
- Digital forms, registration tools, and email campaigns must link to the relevant privacy notice.
- Managers must ensure staff are trained to use the correct notice template based on context.

g. Maintenance and Review

- The DPO maintains the master versions of all privacy notices.

- Notices must be reviewed annually or during a material change in data use or processing systems.

Appendix 5

DPIA Guidelines

Data Protection Impact Assessments (DPIAs) are a legal and operational requirement for assessing the risks associated with personal data processing. They form part of UK Youth's commitment to 'data protection by design and default' under the UK GDPR.

a. What is a DPIA?

A DPIA is a structured risk assessment process used to:

- Identify privacy and data protection risks in a project, product, or initiative
- Assess the likely impact on data subjects' rights and freedoms
- Determine the lawful basis for the processing activity
- Recommend risk mitigation measures or alternative approaches
- Demonstrate accountability and compliance with the UK GDPR

DPIAs are mandatory for any initiative involving high-risk processing activities, including (but not limited to):

- Profiling or scoring individuals
- Use of special category or sensitive personal data
- Large-scale monitoring, tracking, or surveillance
- Automated decision-making, including AI and algorithmic profiling
- Processing of data about children or vulnerable people
- International transfers of personal data (outside the UK/EEA)

Due to their potential legal or ethical implications, projects involving AI, machine learning, facial recognition, or decision-making without human involvement must continually be assessed through a DPIA.

b. When and How to Use a DPIA

A DPIA must be completed:

- ***Before*** the initiative begins (ideally at the design phase)
- Using the UK Youth DPIA Template
- Submitted to the Data Protection Officer (DPO) for review

📌 Before completing a DPIA, use the DPIA Pre-screen Checklist to contact the DPO at data@ukyouth.org.

c. DPIA Process Overview

The DPIA involves seven key steps:

1. **Screening** — Determine if a DPIA is required based on criteria such as scale, sensitivity, profiling, or AI use
2. **Describe the Processing** — Outline what personal data will be collected, used, shared, stored, and deleted
3. **Consultation** — Engage relevant stakeholders (e.g. ICT, safeguarding, legal, programme leads, the DPO)
4. **Assess Necessity and Proportionality** — Explain why the data processing is needed and whether less intrusive methods are possible
5. **Identify and Assess Risks** — Consider risks to individuals' privacy, autonomy, and data rights, especially from automated decisions
6. **Identify Controls** — Propose technical and organisational measures (e.g. encryption, transparency, human review of AI outcomes)
7. **Sign-Off and Monitoring** — The line manager, DPO, and senior manager(s) must formally review and approve the DPIA

d. Roles and Responsibilities

Role	Responsibility
Project Lead	Completes the DPIA and integrates risk controls into the project delivery plan
Line Manager	Reviews DPIA outputs and ensures mitigation actions are practical and implemented
Director	Signs off on any residual risks before go-live
DPO	Provides expert advice, ensures compliance with UK GDPR and AI-specific regulations, and maintains the DPIA record.

e. Documentation and Retention

- Completed DPIAs must be submitted to the DPO at data@ukyouth.org
- DPIAs must be stored securely by the project lead and retained throughout the project lifecycle
- DPIAs must be reviewed periodically, particularly if the initiative involves evolving technologies such as AI or automated decision-making
- If processing changes significantly—especially the use of new decision-making logic or machine learning models—the DPIA must be updated accordingly