# Break Tha Cycle

# UK GDPR Compliance and Data Subject Rights Policy

A practical GDPR policy for lawful, fair, secure and accountable handling of personal information

| | | | |
|---|---|---|---|
| **Document title** | UK GDPR Compliance and Data Subject Rights Policy | **Charity** | Break Tha Cycle |
| **Status** | Approved for use | **Approval date** | 25/06/2026 |
| **Policy owner** | Data Protection Lead / Board of Trustees | **Review due** | 25/06/2027 |
| **Applies to** | Trustees, staff, volunteers, contractors, beneficiaries, participants, parents/carers, partners and visitors, where relevant | **Jurisdiction** | England and Wales unless localised |
| **Related policies** | Data Protection Privacy and Records Management Policy; Safeguarding Policy; Complaints and Feedback Policy; Fundraising and Donations Policy; Social Media and Communications Policy; Volunteer Management Policy; Safer Recruitment DBS and Suitability Checks Policy; Risk Management and Serious Incident Reporting Policy | **Version** | 1.1 |

**Policy summary**

This policy explains how Break Tha Cycle complies with the UK GDPR and Data Protection Act 2018, including lawful basis, individual rights, data sharing, security, breach reporting, retention, privacy information, data protection by design and accountability records.

## 1. Purpose

Break Tha Cycle handles personal information about trustees, staff, volunteers, beneficiaries, participants, young people, parents/carers, donors, supporters, partners, referrers and other people connected with the charity. This policy sets out how the charity will protect that information and meet its obligations under UK data protection law.

This is a standalone UK GDPR policy. It should be read alongside the Data Protection Privacy and Records Management Policy, which covers wider records management and day-to-day filing arrangements. Where this policy sets a stricter requirement, this policy should be followed.

**Policy aim**

Personal information must be collected only when needed, used fairly, shared safely, kept secure, retained only for as long as necessary and made available to individuals when they exercise their legal rights.

## 2. Scope

This policy applies to all personal data processed by Break Tha Cycle, whether held electronically, on paper, in email, messaging apps, cloud systems, spreadsheets, photographs, video, audio, case notes, safeguarding files, referral forms, donor records, incident logs or archived records.

- trustees, employees, sessional workers, volunteers, consultants, contractors and students;
- beneficiaries, young people, adults at risk, parents/carers, family members, donors, supporters, partners, professionals and members of the public;
- information created, received, shared or stored during services, outreach, referrals, safeguarding, fundraising, recruitment, events, communications, social media, training, complaints and governance;
- personal devices or home-working arrangements used for charity business, where authorised;
- third-party systems, processors and partner organisations used to deliver Break Tha Cycle activities.

## 3. Key definitions

| Term | Meaning for Break Tha Cycle |
|---|---|
| **Personal data** | Information relating to an identified or identifiable living person. This includes names, contact details, images, voice recordings, identifiers, opinions, case notes and information that could identify someone when combined with other information. |
| **Special category data** | More sensitive personal data, such as information about health, disability, racial or ethnic origin, religious or philosophical beliefs, sex life, sexual orientation, trade union membership, genetic data or biometric data used for identification. |
| **Criminal offence data** | Information about criminal allegations, proceedings, convictions, cautions, safeguarding concerns involving alleged offences, or related security measures. This needs particular care and a clear legal condition. |
| **Processing** | Anything done with personal data, including collecting, recording, viewing, storing, organising, using, sharing, deleting, anonymising or archiving it. |
| **Controller** | The organisation that decides why and how personal data is processed. Break Tha Cycle is normally a controller for its own charity activities. |
| **Processor** | A supplier or service provider that processes personal data only on Break Tha Cycle's written instructions, such as some cloud software, payroll, mailing or IT providers. |
| **Data subject** | The living person the personal data is about. |
| **Data breach** | A security incident that leads to personal data being accidentally or unlawfully lost, destroyed, altered, disclosed, |

| Term | Meaning for Break Tha Cycle |
|---|---|
| | accessed, sent to the wrong person, made unavailable or compromised. |

## 4. Data protection principles

Break Tha Cycle will build the following principles into every activity involving personal data:

| Principle | What it means in practice |
|---|---|
| **Lawfulness, fairness and transparency** | Use personal data only where there is a lawful basis, treat people fairly and explain clearly how their information will be used. |
| **Purpose limitation** | Collect personal data for specified, explicit and legitimate purposes and do not reuse it in ways that are incompatible with those purposes. |
| **Data minimisation** | Collect and use only the personal data that is adequate, relevant and necessary. Avoid collecting information simply because it might be useful later. |
| **Accuracy** | Take reasonable steps to keep information accurate and up to date, particularly referral, safeguarding, emergency contact, consent and eligibility information. |
| **Storage limitation** | Keep personal data only for as long as needed for the lawful purpose, legal duties, safeguarding, funder requirements, insurance, audit or legitimate charity records. |
| **Integrity and confidentiality** | Use appropriate technical and organisational security measures to protect personal data from unauthorised access, misuse, accidental loss or damage. |
| **Accountability** | Be able to demonstrate compliance through records, policies, privacy information, training, audits, breach logs, data maps and trustee oversight. |

## 5. Roles and responsibilities

| Role | Responsibilities |
|---|---|
| **Board of Trustees** | Has overall responsibility for ensuring Break Tha Cycle complies with data protection law, approves this policy, oversees significant risks and receives reports on serious breaches, high-risk data processing, complaints and audits. |
| **Chair of Trustees** | Ensures data protection concerns are taken seriously and that conflicts, serious incidents or reputational risks are escalated appropriately. |
| **Data Protection Lead** | Coordinates data protection compliance, maintains the data map and key logs, advises staff and volunteers, supports rights requests, reviews data sharing, coordinates breach assessment and reports to trustees. |
| **Designated Safeguarding Lead** | Ensures safeguarding information is recorded, shared and retained lawfully and safely. Works with the Data Protection Lead where data protection and safeguarding duties overlap. |

| Role | Responsibilities |
|---|---|
| **Managers and activity leads** | Make sure people in their team follow this policy, use approved systems, collect only necessary information and report data incidents immediately. |
| **Staff, volunteers and trustees** | Must handle personal information confidentially, follow training, use approved systems, keep records secure, challenge poor practice and report breaches or concerns promptly. |
| **Processors and suppliers** | Must process personal data only under appropriate contractual terms and security arrangements approved by Break Tha Cycle. |
| **Partners and referrers** | Must have a clear reason for sharing information and should agree secure sharing routes and responsibilities before personal data is exchanged. |

**Data Protection Officer note**

Break Tha Cycle will appoint a formal Data Protection Officer only if the law requires one or trustees decide one is needed. Until then, the Data Protection Lead coordinates compliance but does not remove trustee accountability.

# 6. What personal data may be processed

Break Tha Cycle must keep a clear data map showing what personal data is processed, where it comes from, why it is needed, who can access it, who it is shared with, how long it is kept and how it is protected.

| Area | Examples of personal data | Typical purpose |
|---|---|---|
| Beneficiaries and participants | Name, age/date of birth, contact details, emergency contacts, referral information, attendance, support needs, safeguarding notes, behaviour/support plans, outcomes and feedback. | To assess eligibility, deliver safe support, make reasonable adjustments, monitor outcomes, manage risk and meet safeguarding duties. |
| Children and families | Parent/carer details, consent forms, school/referrer details, SEN/SEND information, health or accessibility needs, incident records and authorised collection arrangements. | To deliver age-appropriate support, communicate with parents/carers, manage safeguarding and provide inclusive activities. |
| Trustees, staff and volunteers | Application details, references, identity and right-to-work checks where relevant, DBS information, training, supervision, payroll/expenses, emergency contacts and conduct records. | To recruit safely, manage roles, meet legal obligations, support people and protect beneficiaries. |
| Donors and supporters | Contact details, donation history, Gift Aid declarations, communication preferences and fundraising interactions. | To process donations, thank supporters, meet financial and tax requirements and communicate lawfully. |
| Partners and professionals | Contact details, role, organisation, referral notes, meeting records and information sharing decisions. | To coordinate services, make referrals, manage partnerships and keep an audit trail. |
| Images, video and stories | Photos, video, audio, quotations, case studies, social media comments and publicity consent records. | To promote the charity, report impact and communicate safely, only where appropriate consent or another lawful basis applies. |

# 7. Lawful basis for processing

Personal data must not be collected or used unless Break Tha Cycle has identified a lawful basis. The lawful basis must be recorded in the data map or a specific processing record before the processing starts.

| Lawful basis | When Break Tha Cycle may use it |
|---|---|
| **Consent** | Use where the person has a genuine choice and can withdraw consent without detriment. Suitable for many photos, newsletters, non-essential communications and optional activities. Not usually suitable where support depends on processing or there is an imbalance of power. |
| **Contract** | Use where processing is necessary for a contract or to take steps before entering a contract, such as employment, consultancy or venue booking arrangements. |
| **Legal obligation** | Use where the charity must process data to comply with the law, such as some employment, tax, accounting, health and safety or safeguarding-related obligations. |
| **Vital interests** | Use in an emergency where processing is necessary to protect someone's life or physical safety and they cannot give consent. |
| **Public task** | Usually less common for Break Tha Cycle unless carrying out a specific task in the public interest or under official authority. Seek advice before relying on this basis. |
| **Legitimate interests** | Use where the processing is necessary for the charity's legitimate interests or the legitimate interests of others, and these are not overridden by the rights and interests of the person. A legitimate interests assessment should be recorded for higher-risk uses. |

# 8. Special category and criminal offence data

Special category and criminal offence data require extra safeguards. Break Tha Cycle must identify both a lawful basis under UK GDPR Article 6 and an additional condition for special category or criminal offence data where required.

- collect sensitive information only where it is needed for safeguarding, wellbeing, reasonable adjustments, equality monitoring, employment, risk management or another clear lawful purpose;
- restrict access to those who need to know and keep sensitive information in secure folders or approved systems;
- avoid recording excessive detail, speculation, gossip or personal opinions that are not relevant to the purpose;
- separate safeguarding records from general programme records where this is necessary to protect confidentiality;
- use anonymised or aggregated information for reporting wherever possible;
- seek advice before sharing criminal offence data, detailed health information, exploitation concerns or highly sensitive family circumstances outside agreed safeguarding or legal routes.

**Safeguarding and data protection**

Data protection law does not prevent appropriate safeguarding information sharing. Staff and volunteers must never promise absolute confidentiality where someone may be at risk of harm. Information sharing must still be necessary, proportionate, relevant, accurate, timely and secure.

# 9. Privacy information and transparency

Break Tha Cycle will provide clear privacy information so people understand how their personal data will be used. Privacy information should be concise, easy to understand and available before or at the point information is collected, unless an exemption or safeguarding consideration applies.

- who Break Tha Cycle is and how to contact the charity or Data Protection Lead;
- what information is collected and where it comes from;
- why the information is needed and the lawful basis for processing;
- who the information may be shared with, including safeguarding, professional, statutory, funder, insurer or processor recipients where relevant;
- how long information is kept or how retention decisions are made;
- the individual's data protection rights and how to use them;
- how to complain to Break Tha Cycle and the Information Commissioner's Office;
- whether any automated decision-making, profiling, overseas transfer or optional marketing is involved.

# 10. Consent

Consent must be freely given, specific, informed and unambiguous. Consent is not valid where a person feels they have no real choice or where refusing would unfairly affect access to support. Consent should not be bundled into general terms or assumed from silence.

1. Use clear wording that explains exactly what the person is agreeing to.
2. Record who gave consent, when, how, what they were told and how they can withdraw it.
3. Provide separate consent choices for different purposes, such as photography, newsletters, case studies and optional partner contact.
4. Respect withdrawal of consent promptly unless another lawful basis requires continued processing.
5. Review consent when the purpose changes, a child grows older, a service changes, or the original consent is no longer clear or current.

For children and young people, staff must consider age, understanding, parental responsibility, safeguarding context and the nature of the activity. Where there is doubt, seek advice from the Data Protection Lead and Designated Safeguarding Lead.

# 11. Data protection by design and default

Data protection must be considered at the start of new projects, not added at the end. Break Tha Cycle will assess privacy risks before introducing new systems, referral routes, monitoring tools, online platforms, photography projects, partnership arrangements, funder reporting processes or high-risk services.

- collect the minimum data needed for the purpose;
- use privacy-friendly default settings in systems and forms;
- limit access by role and remove access quickly when someone leaves or changes role;
- use secure systems rather than personal email, informal messaging or unsecured spreadsheets wherever possible;
- avoid publishing identifiable stories, images or locations where there is safeguarding, domestic abuse, exploitation, immigration, community safety or stigma risk;
- complete a Data Protection Impact Assessment screening where processing may be high risk.

# 12. Data Protection Impact Assessments

A Data Protection Impact Assessment, often called a DPIA, is a structured risk assessment for high-risk processing. Break Tha Cycle will complete DPIA screening before starting activities likely to create a high risk to people's rights and freedoms.

| DPIA trigger | Examples for Break Tha Cycle |
|---|---|
| New technology or system | New case-management system, cloud platform, app, AI tool, online referral portal or digital monitoring process. |
| Sensitive or vulnerable groups | New work involving children, adults at risk, trauma, exploitation, violence, mental health, disability, immigration or criminal justice information. |
| Large-scale or systematic monitoring | Regular online monitoring, CCTV/audio recording, tracking attendance patterns across multiple services or profiling risk levels. |
| Data matching or new sharing | Combining information from schools, police, social care, health, funders or community partners in a new way. |
| Public communication risk | Using case studies, photos, film or social media where people could be identified and harmed. |

The Data Protection Lead will coordinate DPIAs with the relevant activity lead and, where safeguarding is involved, the Designated Safeguarding Lead. Trustees must review unresolved high risks before the activity begins.

## 13. Data subject rights

Individuals have rights over their personal data. These rights are not absolute and may depend on the circumstances, legal basis, safeguarding issues and exemptions. Break Tha Cycle will respond fairly, promptly and within legal timescales.

| Right | Break Tha Cycle response |
|---|---|
| **Right to be informed** | People should receive clear privacy information about how their data is used. |
| **Right of access** | People can request a copy of their personal data and related information. This is often called a subject access request. |
| **Right to rectification** | People can ask for inaccurate information to be corrected or incomplete information to be completed. |
| **Right to erasure** | People can ask for personal data to be deleted in certain circumstances. The charity may need to keep information where there is a legal, safeguarding, financial or legitimate reason. |
| **Right to restrict processing** | People can ask the charity to limit how their data is used in certain circumstances. |
| **Right to data portability** | People can ask for certain data they provided to be supplied in a structured, commonly used, machine-readable format where the right applies. |
| **Right to object** | People can object to certain processing, including some processing based on legitimate interests or direct marketing. |
| **Rights about automated decision-making and profiling** | People have rights where decisions are made solely by automated means and have legal or similarly significant effects. Break Tha Cycle will not use solely automated high-impact decisions unless trustees approve a lawful and safeguarded process. |

# 14. Handling data subject rights requests

A rights request does not have to mention GDPR or use a specific form. It can be made verbally, in writing, by email, by message, through a representative or during a meeting. Anyone receiving a request must send it to the Data Protection Lead on the same working day wherever possible.

6. Log the request immediately, including the date received, requester details, the right being exercised and how the request was made.
7. Acknowledge the request and explain any identity checks or clarification needed. Do not request unnecessary identity documents.
8. Confirm whether the requester is the data subject, a person with parental responsibility, an authorised representative, a solicitor, advocate or statutory body.
9. Search all relevant systems, emails, paper files, archives, incident logs and staff-held records that may contain the requester's personal data.
10. Review the information for third-party data, safeguarding risk, legal privilege, confidential references, management information, exemptions or information that may cause serious harm if disclosed.
11. Prepare the response in clear language. Provide information securely and in an accessible format where reasonably possible.
12. Respond within one month unless the law allows an extension. Any extension must be approved by the Data Protection Lead and explained to the requester.
13. Record the outcome, information provided or refused, reasons for any refusal, exemptions relied on, dates and any follow-up actions.

**Safeguarding check before disclosure**

Before disclosing information from safeguarding, behaviour, SEN/SEND, complaint or incident records, the Data Protection Lead must consider whether disclosure could put a child, adult at risk, survivor, witness, staff member, volunteer or third party at risk of harm.

# 15. Data sharing

Break Tha Cycle will share personal data only where there is a clear purpose, lawful basis and secure method. Sharing should be necessary, proportionate and recorded. Staff must not share personal information casually, by insecure channels or because another organisation asks for it without a clear reason.

- confirm who is requesting the information and their authority to receive it;
- check what information is needed and avoid sharing excessive detail;
- identify the lawful basis and any special category/criminal offence condition;
- consider whether consent is required or whether another basis is more appropriate;
- consider safeguarding, safety, confidentiality, equality and reputational risks;
- use secure transfer methods, such as encrypted email, secure portal, password-protected files with separately shared passwords, or approved systems;
- record what was shared, with whom, when, why, how and who authorised it.

| Sharing type | Expected control |
|---|---|
| **Routine internal sharing** | Information shared within Break Tha Cycle must be limited to people who need it for their role. |
| **Safeguarding sharing** | Information may be shared with statutory agencies, safeguarding partners, police, social care, health or schools where necessary to protect someone from harm. |
| **Partner referrals** | Referral information should be shared under agreed referral pathways with clear privacy information and secure routes. |
| **Funder reporting** | Use anonymised or aggregated data wherever possible. Identifiable information must not be shared with funders unless there is a lawful basis and clear notice. |

| Sharing type | Expected control |
|---|---|
| **Professional advice** | Legal, HR, safeguarding, insurance or audit advisers may receive information where necessary and subject to confidentiality arrangements. |
| **Publicity and stories** | Use identifiable images, names or stories only where lawful, safe and approved under the Social Media and Communications Policy. |

## 16. Processors, suppliers and cloud systems

Before a supplier processes personal data for Break Tha Cycle, the charity must complete proportionate due diligence and ensure suitable written terms are in place. This applies to cloud storage, email systems, case management, payroll, accounting, mailing lists, event platforms, survey tools, IT support, external consultants and hosted databases.

- what data the processor will handle and why;
- security measures, access controls, encryption, backups and incident response arrangements;
- where data will be stored and whether any international transfer is involved;
- confidentiality obligations for supplier staff;
- sub-processors and how changes will be notified;
- support for data subject rights and deletion/return of data at the end of the contract;
- breach notification duties and timescales;
- audit, assurance or certification evidence appropriate to the risk.

## 17. International transfers

Break Tha Cycle must check whether personal data is transferred outside the UK when using cloud systems, online platforms, overseas suppliers, international partners or global support desks. International transfers may occur even where the charity itself is based in the UK.

The Data Protection Lead must confirm that an appropriate transfer safeguard or adequacy arrangement is in place before personal data is transferred outside the UK. Higher-risk transfers must be escalated to trustees or specialist advice.

## 18. Security and confidentiality

Everyone working with Break Tha Cycle must protect personal data from unauthorised access, loss, theft, accidental disclosure, damage and misuse. Security measures must be proportionate to the sensitivity and volume of information and the harm that could result from misuse.

| Control area | Minimum expectation |
|---|---|
| Access control | Use individual accounts where possible, strong passwords, multi-factor authentication where available, role-based access and prompt removal of access when someone leaves. |
| Devices | Use password/PIN protected devices, keep software updated, enable device encryption where possible and avoid storing charity data on unapproved personal devices. |
| Email and messaging | Check recipients before sending, avoid group disclosure, use BCC where appropriate, do not send sensitive records through insecure channels and report misdirected emails immediately. |
| Paper records | Keep paper records locked away, do not leave them visible in vehicles or public places, transport them securely and dispose of them by confidential shredding. |

| Control area | Minimum expectation |
|---|---|
| Remote working | Work in private where possible, avoid public Wi-Fi for sensitive work unless using approved protection, keep family/household members from viewing records and store papers securely. |
| Photos and media | Store images securely, label consent restrictions, avoid unnecessary geolocation information and remove images where consent is withdrawn or safeguarding risk changes. |
| Backups and recovery | Use approved systems with reliable backup arrangements. Important charity records must not exist only on one person's device or inbox. |
| Training and awareness | Provide induction and refresher training proportionate to role and risk. |

## 19. Data retention and disposal

Personal data must not be kept indefinitely. Retention periods must be based on legal duties, safeguarding needs, charity governance, financial and tax requirements, insurance, funder terms, audit requirements and operational need. Where the retention period is unclear, the Data Protection Lead must agree a proportionate period with the relevant policy owner.

- keep a retention schedule covering beneficiary records, safeguarding files, referral records, consent forms, volunteer/staff files, trustee records, financial records, donor records, complaints, accidents/incidents and marketing preferences;
- mark files with closure dates and planned review/deletion dates where possible;
- archive only what is needed and restrict access to closed sensitive files;
- delete duplicate, draft and working copies when no longer needed;
- dispose of paper records by confidential shredding and delete electronic records securely;
- pause deletion where records are needed for a complaint, safeguarding review, legal claim, investigation, audit or subject access request.

## 20. Personal data breaches

All suspected or actual personal data breaches must be reported immediately to the Data Protection Lead. Breaches must not be hidden, delayed or handled informally. Quick reporting allows the charity to protect people and meet legal timescales.

| Stage | Action |
|---|---|
| 1. Report | Tell the Data Protection Lead as soon as possible. Include what happened, when, whose data is involved, who has seen it and any immediate action already taken. |
| 2. Contain | Recover data if possible, recall emails, disable links, change passwords, isolate affected systems, retrieve papers or ask unintended recipients to delete securely. |
| 3. Assess risk | Assess the likelihood and severity of harm, considering sensitivity, volume, vulnerability, safeguarding risk, identity theft, financial loss, distress, discrimination or reputational harm. |
| 4. Decide notifications | If a risk to people's rights and freedoms is likely, notify the ICO as soon as possible and where feasible within 72 hours. If high risk, notify affected individuals without undue delay. |
| 5. Record | Record all breaches, including those not reported to the ICO, with reasons, decisions and evidence. |
| 6. Learn | Identify root causes, update controls, brief staff/volunteers and report significant learning to trustees. |

**Breach examples**

Lost paperwork, an email sent to the wrong recipient, unauthorised access to a case file, stolen device, insecure public link, ransomware, accidental disclosure in a group email, lost notebook, incorrect social media post, or a volunteer retaining records after leaving may all be personal data breaches.

## 21. Direct marketing, fundraising and communications

Fundraising, supporter communications and newsletters must follow this policy, the Fundraising and Donations Policy, the Social Media and Communications Policy and any additional rules that apply to electronic marketing. Communication preferences must be recorded and respected.

- use clear opt-in wording for optional newsletters, fundraising updates or marketing where consent is required;
- do not add people to marketing lists simply because they used a service, attended an event or made a referral;
- make unsubscribing or changing preferences easy and prompt;
- screen fundraising stories, photos and quotes for safeguarding and dignity risks;
- use anonymised impact information unless identifiable stories are lawful, safe and agreed;
- keep suppression lists where needed to ensure people are not contacted again after opting out.

## 22. Photos, video, case studies and social media

Identifiable photos, videos, audio recordings and stories can create safeguarding, privacy and dignity risks. The charity must be particularly careful when working with children, adults at risk, people affected by violence, exploitation, trauma, immigration concerns, criminal justice issues or family conflict.

14. Explain the intended use clearly before taking or using the material.
15. Record consent or other lawful basis, restrictions and expiry/review dates.
16. Avoid using full names, school names, locations or details that could identify or endanger someone unless necessary and approved.
17. Check again before using old images or stories in a new context.
18. Remove or stop using material where consent is withdrawn, safeguarding risk changes or continued use would be unfair.

## 23. Training and awareness

All trustees, staff and volunteers must receive data protection guidance appropriate to their role. People with access to sensitive records must receive more detailed training. Training should be refreshed when roles change, systems change, incidents happen or at least every two years.

- what personal data is and why it matters;
- confidentiality and secure record handling;
- how to recognise and report a personal data breach;
- how to identify a data subject rights request;
- safe email, device, cloud and paper record practices;
- safeguarding information sharing and the limits of confidentiality;
- photo, story and social media privacy rules.

## 24. Complaints and concerns

Anyone may raise a concern about how Break Tha Cycle handles personal data. Concerns should be directed to the Data Protection Lead or handled under the Complaints and Feedback Policy where appropriate. The

charity will take concerns seriously, investigate proportionately, correct errors where needed and explain the outcome.

People also have the right to complain to the Information Commissioner's Office. Break Tha Cycle will cooperate with the ICO and will preserve records relevant to any complaint, investigation or regulatory contact.

## 25. Monitoring, audit and trustee reporting

The Data Protection Lead will provide proportionate reports to trustees at least annually and sooner if a serious issue arises. Reports should focus on risk, compliance and improvement, not unnecessary personal detail.

- data breaches and learning actions;
- data subject rights requests and response times;
- DPIAs completed or pending;
- changes to processing activities, systems, suppliers or data sharing;
- training completion and awareness needs;
- privacy notices, retention schedule and data map updates;
- complaints or ICO contact related to data protection.

# Appendix A - Lawful basis record template

Use this template when adding a new type of processing to the data map or when reviewing an existing activity.

| Question | Record |
|---|---|
| Processing activity | |
| Whose personal data is involved? | |
| What categories of personal data are involved? | |
| Purpose of processing | |
| Lawful basis under Article 6 | |
| Special category or criminal offence condition, if applicable | |
| Why the processing is necessary | |
| Privacy information provided | |
| Who can access the data | |
| Who data is shared with | |
| Retention period | |
| Security controls | |
| Owner and review date | |

# Appendix B - Data subject rights request log

| Date received | Requester | Right/request | Deadline | Owner | Outcome/notes |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Keep copies of request correspondence, identity checks, searches performed, exemptions considered, information disclosed and final response securely with the rights request record.

# Appendix C - Subject access request checklist

| Step | Completed / notes |
|---|---|
| Request logged with date received and deadline calculated | |
| Identity and authority checked proportionately | |
| Scope clarified if needed | |
| Relevant systems, paper files, emails and archives searched | |
| Third-party information identified and assessed | |
| Safeguarding/harm risks assessed before disclosure | |
| Exemptions considered and recorded if information withheld | |
| Response prepared in accessible format | |
| Information sent securely | |
| Outcome recorded and learning action noted | |

# Appendix D - Personal data breach assessment form

| Field | Details |
|---|---|
| Date/time discovered | |
| Reported by | |
| What happened? | |
| Type of data involved | |
| Number and type of people affected | |
| Immediate containment action | |
| Likelihood of harm | Low / Medium / High - reasons: |
| Severity of harm | Low / Medium / High - reasons: |
| ICO notification required? | Yes / No - reasons: |
| Affected individuals notification required? | Yes / No - reasons: |
| Other notifications | Insurer / NCSC / police / partner / funder / Charity Commission - reasons: |
| Root cause | |
| Learning and prevention action | |
| Trustee notification and date | |
| Closed by and date | |

# Appendix E - DPIA screening checklist

Complete this screening before new processing starts. If any answer indicates high risk, complete a full DPIA and seek advice where needed.

| Question | Yes/No/Notes |
|---|---|
| Will we process special category, criminal offence, safeguarding or highly sensitive personal data? | |
| Will the activity involve children, adults at risk or people in vulnerable circumstances? | |
| Will we use new technology, AI, tracking, monitoring, profiling or automated decision-making? | |
| Will we share data with a new partner, public body, funder or supplier? | |
| Will data be stored or accessed outside the UK? | |
| Could misuse of the data cause harm, distress, discrimination, financial loss or safeguarding risk? | |
| Can we reduce the amount of identifiable data or use anonymised information? | |
| Have privacy information, security controls and retention arrangements been agreed? | |
| Does the activity need trustee review before launch? | |

# Appendix F - Data sharing and processor checklist

| Check | Record |
|---|---|
| Name of organisation/supplier/partner | |
| Controller, joint controller or processor relationship | |
| Purpose of sharing or processing | |
| Data categories involved | |
| Lawful basis and condition for sensitive data, if relevant | |
| Privacy information given to individuals | |
| Security method for sharing/access | |
| Written agreement, contract or sharing protocol in place | |
| International transfer check completed | |
| Retention/deletion arrangements agreed | |
| Breach notification arrangements agreed | |
| Review date and owner | |

# Appendix G - Annual GDPR compliance checklist

| Area | Evidence / action needed |
|---|---|
| Data map reviewed and updated | |
| Privacy notices checked and published/shared appropriately | |
| Retention schedule reviewed and disposal completed where due | |
| Data subject rights log reviewed for timeliness and learning | |
| Breach log reviewed and controls improved | |
| DPIAs completed for high-risk activities | |
| Suppliers/processors reviewed and contracts checked | |
| Marketing and consent records reviewed | |
| Access permissions reviewed and leavers removed | |
| Training completed by trustees, staff and volunteers | |
| Trustee report completed and actions assigned | |

# Review and approval record

| Version | Approved by | Approval date | Main changes | Next review |
|---|---|---|---|---|
| 1.1 | Board of Trustees | 25/06/2026 | New standalone policy approved for use. | 25/06/2027 |
| | | | | |
| | | | | |

# Guidance and source materials

This policy should be reviewed against the latest official guidance whenever Break Tha Cycle changes its activities, works with a new beneficiary group, enters a new partnership or receives a serious complaint or incident.

- Information Commissioner's Office - UK GDPR data protection principles: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/
- Information Commissioner's Office - Individual rights: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/
- Information Commissioner's Office - Personal data breach reporting: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- Information Commissioner's Office - Accountability and governance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/
- Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents
- UK GDPR: https://www.legislation.gov.uk/eur/2016/679/contents

This policy is an adoption draft for Break Tha Cycle. Trustees should review it against the charity's actual systems, privacy notices, retention schedule, contracts, safeguarding pathways and ICO registration position before publication or use.