Bridging the Gap (Manchester)

General Data Protection Policy (GDPR)

(fully updated for UK GDPR, DPA 2018 and DPDI Act 2024-25)

Registered Charity Number: 1170952

This policy and guidance will be reviewed in line with any governmental changes in relation to General Data Protection Regulation (GDPR): Data Protection or when incidents dictate. This will ensure that this document is current and fit for purpose.

Date last reviewed: 16th September 2024 & 19 January 2026
Reviewed by: Michelle McHale
Next review date:19th January 2027

This policy should be read in conjunction with the following Bridging the Gap policies: -

- Safeguarding Policy & Procedure
- Privacy Policy
- Acceptable Use of IT & Telephony Equipment Policy & Guidance
- Disciplinary Policy & Procedure
- Social Media Usage Policy & Procedure
- Cyber Security Policy & Procedure
- Data Privacy Statements

Contents:

1. Purpose

Bridging the Gap (Manchester) (BTG) is committed to protecting the personal data of its clients, volunteers, staff, trustees, referrers, contractors, partner organisations and visitors. This policy sets out how BTG complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Protection and Digital Information Act (DPDI Act 2024-25)
- ICO guidance and statutory codes of practice

This policy applies to all personal data processed by BTG, regardless of format or storage location, and includes data processed by contractors and partner organisations acting on BTG's behalf.

BTG recognises its accountability obligations under UK GDPR and the DPDI Act. BTG must not only comply with data protection law but also be able to demonstrate compliance through clear governance, documented decisions, and robust organisational measures.

2. Key Definitions (2025)

- **Personal data** - information identifying a living individual, including digital identifiers recognised under the DPDI Act.
- S**pecial category data** - sensitive data requiring additional protection (e.g. health, ethnicity, beliefs, biometrics used for identification).
- **Processing** - any operation performed on personal data.
- **Data subject** - the individual to whom the data relates.
- **Data controller** - BTG, which determines how and why data is processed.
- **Data processor** - a third party processing data on BTG's behalf
- **Data Protection Officer (DPO)** - person responsible for monitoring, compliance and reporting
- **Automated decision making** - decisions made solely by automated means, including AI systems, that have legal or significant effects.
- **Personal data breach** - unauthorised access, disclosure, loss, alteration or destruction of personal data.
- **International transfer** - sending or storing personal data outside the UK, including cloud-based storage.
- **Recognised legitimate interests –** specific purposes identified in the Data Protection and Digital Information Act (DPDI Act 2024–25) where organisations may rely on legitimate interests **without needing to complete a balancing test**. These include safeguarding, crime prevention, network and information security, and other purposes designated in legislation or ICO guidance.

3. Principles of Data Protection

BTG processes personal data in accordance with the following principles:

- **Lawfulness, fairness and transparency** – data must be processed lawfully, fairly and in a way that is clear to individuals.
- **Purpose limitation** – data must be collected for specified, explicit and legitimate purposes and not used in ways incompatible with those purposes.
- **Data minimisation** – data must be adequate, relevant and limited to what is necessary for the intended purpose.
- **Accuracy** – data must be accurate and kept up to date.

- **Storage limitation** – data must be retained only for as long as necessary.
- **Integrity and confidentiality** – data must be processed securely to protect against unauthorised or unlawful access, loss, destruction or damage.
- **Accountability** – BTG must be able to demonstrate compliance with all data protection principles through documented decisions, governance and organisational measures.

These principles reflect the requirements of the UK GDPR and the strengthened accountability duties introduced under the DPDI Act.

4. Data Controller

BTG is the data controller for all personal data it processes. The Board of Trustees holds overall accountability. BTG is registered with the ICO (Registration No; ZA294550). BTG reviews its ICO registration annually.

The ICO exists to empower people through information and is the independent supervisory body regarding the UK's data protection legislation. The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

4.1 Data Processor

BTG's Foodbank service provision is franchised to Trussell. BTG as a data controller works with Trussell who processes anonymised data on behalf of BTG. This data is used for research and campaigning purposes to raise awareness of foodbank use and paths out of poverty. A written data processing agreement is in place.

5. Roles and Responsibilities

5.1 Trustees

- Ensure BTG complies with data protection law.
- Oversee risk management and governance

5.2 Data Protection Officer (DPO)

- Monitor compliance and oversee implementations of the policy.
- Advise on DPIAs and AI-risk assessments.
- Act as the primary contact for data subjects and the ICO
- Report annually to the Trustee Board.

DPO Contact Details:

Name: Jennifer Uisobo
Email: Jennifer@manchestersouthcentral.foodbank.org.uk
Telephone: 0161 226 3413

5.3 Project Manager

- Acts as the organisational representative.
- Ensures day-to-day compliance.

5.4 All Staff

- Process personal data lawfully and securely.
- Follow BTG's data protection procedures.
- Report concerns or breaches immediately to the DPO.
- Seek advice before collecting new data, sharing data externally, or relying on consent.
- Notify BTG of changes to their own personal data.

6. Lawful Processing of Personal Data

6.1 Lawful Bases (2025 update)

BTG will only process personal data where one of the following applies:

- **Contract** - necessary to enter into or perform a contract.
- **Legal obligation** - required by law
- **Vital interests** - necessary to protect life.
- **Public task** - necessary to perform a task in the public interest.
- **Legitimate interests** - necessary for BTG's legitimate aims, balanced against individual rights.
- **Consent -** freely given, specific, informed and unambiguous.

Under the DPDI Act, BTG may rely on "recognised legitimate interests" without a balancing test, including:

- Safeguarding
- Crime prevention
- Network and information security

6.2 Special Category Data

BTG will only process special category data where an additional condition under UK GDPR and the DPA 2018 applies.

6.3 Data Minimisation and Accuracy

BTG will:

- Collect only what is necessary
- Keep data accurate and up to date
- Review data regularly
- delete or anonymise data when no longer required.

6.4 Privacy Notices

BTG provides clear privacy notices explaining:

- What data is collected
- Why it is collected
- How it is used
- Who it is shared with
- How long it is kept
- Rights of individuals
- Whether AI-assisted processing is used
- Whether data is transferred internationally

7. Sharing Personal Data

BTG may share personal data where:

- Necessary to safeguard individuals or staff
- Required to deliver services
- Required by law (e.g., crime prevention, HMRC, safeguarding)
- Necessary for emergency response
- With contractors who meet 2025 ICO “appropriate safeguards” standards
- With local authorities or statutory partners where necessary to fulfil safeguarding duties, support service delivery, or comply with legal obligations

BTG will:

- Use written data-sharing agreements
- Share only what is necessary
- Ensure third parties provide adequate security
- Conduct due diligence on processors

International transfers will use ICO approved mechanisms.

8. Rights of Individuals

8.1 Subject Access Requests (SARs)

Individuals may request:

- Confirmation that their personal data is processed
- Access to their data
- Information about processing purposes, recipients, retention and sources

Requests may be made verbally or in writing. Staff must forward any SAR to the DPO immediately.

8.2 Responding to SARs

BTG will:-

- Verify identity
- Respond within one month (extendable to three months for complex requests)
- Provide information free of charge unless the request is manifestly unfounded or excessive
- Withhold information where disclosure would cause serious harm or is legally restricted
- Apply lawful exemptions where appropriate, including management forecasting, legal privilege, negotiations, and other exemptions permitted under data protection legislation

8.3 Other Rights

Individuals may also:

- Withdraw consent
- Request rectification, erasure or restriction
- Object to processing
- Request data portability
- Challenge automated or AI-assisted decision making
- Be informed of high-risk data breaches
- Complain to the ICO

Requests must be referred to the DPO.

9. Photographs and Videos

BTG will obtain written consent before using images for communication or promotional purposes. Images used for identification may constitute biometric data and require additional safeguards. Consent may be withdrawn at any time. Images will be retained only for as long as necessary for the purpose for which they were collected and will be deleted or securely archived in line with BTG's retention schedule.

10. Data Protection by Design (2025 update)

BTG will:

- Integrate data protection into all processing activities
- Conduct Data Protection Impact Assessments (DPIAs) where required
- Ensure DPIAs are mandatory for high‑risk processing
- Conduct AI-risk assessments for automated or AI-assisted processing
- Maintain Records of Processing Activities (ROPAs)
- Use privacy-enhancing technologies where appropriate
- Review and update policies regularly
- Train staff annually

11. Data Security

BTG will protect personal data through:

- Secure storage of paper and electronic records
- Multi-factor authentication for systems containing personal data
- Encryption of portable devices
- Strong passwords and access controls

- Restricted access to shared drives
- Immediate removal of access when staff or trustees leave
- Secure configuration of cloud-based systems, ensuring data is stored on UK-based servers or in locations offering adequate protection under UK data protection law
- Mandatory reporting of suspected breaches

12. Retention and Disposal

BTG will:

- Retain data only as long as necessary
- Follow documented retention schedules
- Ensure all retention decisions align with BTG's Retention Schedule, which sets out specific time periods for each category of data
- Dispose of data securely (shredding, secure deletion)
- Ensure third-party disposal providers meet ICO standards

13. Personal data breaches

BTG will:

- Report suspected breaches immediately to the DPO
- Investigate and contain breaches
- Assess risks to individuals
- Notify the ICO within 72 hours where required
- Notify affected individuals where risk is high
- Document all breaches and decisions
- Review incidents to prevent recurrence

Non-compliance may result in disciplinary action, In line with BTG's Disciplinary Policy

14. Training

All staff and trustees receive:

- Induction training
- Annual data protection training
- Updates on legislative or procedural changes
- Cyber-security and SAR-handling training

Volunteers are encouraged to complete GDPR training via Trussell. Training records are maintained by the Project Managers.

15. Monitoring and Review

The DPO monitors compliance and reviews this policy annually or sooner if legislation or ICO guidance changes. The updated policy is shared with the Board of Trustees for approval.

Appendix 1: Personal Data Breach - Quick Reference Flowchart (2025)

1. Breach Suspected

    - Identify the incident loss, theft, unauthorised access, mis-send, cyber incident, human error.
    - Stop further data loss - retrieve device, lock account, isolate system.
    - Report immediately to the DPO. Do not investigate alone.

2. DPO Initial Response

    - Confirm whether a breach has occurred - Assess what happened and what data is involved.
    - Secure the situation - Change passwords, revoke access, recover data if possible.
    - Log the incident - Record facts, time, people involved.

3. Containment & Mitigation

    - Limit the impact - Disable accounts, isolate systems, contact IT support.
    - Preserve evidence - Keep emails, screenshots, logs

4. Risk Assessment

    - Assess harm to individuals - identity theft, financial loss, discrimination, distress, safeguarding risk.
    - Assess sensitivity of data - special category, financial, safeguarding, contact details.

5. ICO Notification Decision

    - Is there a risk to individuals' rights and freedoms? if yes, notify ICO within 72 hours
    - Prepare ICO report - Nature of the breach, data affected, consequences, actions taken.

6. Notify Individuals (If High Risk)

    - Inform affected people promptly _ Explain what happened, risks, and what they should do.
    - Provide DPO contact details - Offer support and guidance.

7. Documentation

    - Record everything - Facts, decisions, actions, timeliness, outcomes
    - Store securely in breach log, required for ICO accountability

8. Review and Improve

    - Conduct a post incident review - Identify root causes and lessons learned.
    - Update procedures and training
    - Strengthen controls to prevent recurrence

Appendix 2: Personal Data Breach Reporting Form

Section 1: Reporter Details

- Name:_____
- Role: _____
- Date & Time of Report: _____
- Contact Details: _____

Section 2: Incident Details

2.1 Date & Time Incident Occurred / Discovered: _____

2.2 Location of incident: _____

2.3 How was the incident discovered? _____

2.4 Describe What Happened (facts only) _____

_____

_____

Section 3: Data Involved

3.1 Type of data affected: (tick all that apply)

☐ Contact Details
☐ Financial Information
☐ Special category data (health, ethnicity, beliefs, etc…)
☐ Safeguarding Information
☐ Identification Documents
☐ Digital Identifiers / Login Credentials
☐ Other: _____

3.2 Approximate number of individuals affected: _____

3.3 Is the data identifiable?

☐ Yes
☐ No
☐ Unsure

3.4 Was the data encrypted or otherwise protected?

☐ Yes

☐ No
☐ Partially
☐ Details: _____

Section 4: Immediate Actions Taken

4.1 Steps taken to contain or limit the breach: _____

4.2 Has the data been recovered?

☐ Yes
☐ No
☐ Partially

4.3 Has access been revoked / Passwords changed

☐ Yes
☐ No
☐ N/A

Section 5: People Involved

5.1 Names of Staff / volunteers involved (if relevant):

☐
☐
☐

5.2 Names of any external parties involved:

☐
☐
☐

Section 6: Potential Impact

Possible consequences for individuals: (tick all that apply)

☐ Identity theft
☐ Financial Loss
☐ Emotional Distress
☐ Discrimination
☐ Safeguarding Risk
☐ Reputational Harm
☐ Other: _____

Additional notes on potential harm:

Section 7: For DPO Use Only (to be completed by the Data Protection Officer)

Assessment

7.1 Is this a personal data breach under GDPR?

☐ Yes
☐ No

7.2 Risk Level:

☐ Low
☐ Medium
☐ High

7.3 ICO notification required?

☐ Yes
☐ No

If yes, date / time reported: _____

7.4 Individuals need to be notified?

☐ Yes
☐ No

If yes, date / time notified: _____

Action Taken:

☐
☐
☐

Follow Up Required:

☐
☐
☐

DPO Name & Signature

Name:
Signature:
Date: