Bridging the Gap (Manchester)

General Data Protection Regulation: Data Protection Policy

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: 23rd January 2023
Reviewed by: Lynda Mason & Michelle McHale
Next review date: 23rd January 2024

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

- **Safeguarding Policy**
- **Privacy Policy**
- **IT Acceptable Use of IT & Telephony Equipment Policy**
- **Disciplinary Policy**
- **Social Media Usage Policy**

Contents:

1. Aims

Bridging the Gap (Manchester) (BTG) aims to ensure that all personal data collected about staff, volunteers, trustees, clients, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation 2018 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

Digital technology has transformed almost every aspect of our lives. The Data Protection Act 2018 aims to: -

- make the UK's data protection laws fit for the digital age at at time when an ever increasing amount of data is being processed
- empower people to take control of their own data
- support UK businesses and organisations
- ensure that the UK was prepared for the future after the UK left the EU.

This policy meets the requirements of the GDPR 2018 and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

Organisations found to be in breach of the General Data Protection Regulations can be very heavily fined.

Protection Principles

The GDPR is based on data protection principles that BTG must comply with.

The key principles say that personal data must be: -

- collected and processed lawfully, fairly and in a transparent manner. It must be relevant and not excessive
- collected for specified, explicit and legitimate purposes and used only for the reasons it was collected
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- kept accurate and up-to-date and corrected or deleted if there are mistakes
- kept for no longer than is necessary for the purposes for which it is processed

- processed in accordance with people's rights kept safe to protect it from being lost, stolen or used inappropriately.

This policy sets out how BTG aims to comply with these principles.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: - ● Name (including initials) ● Contact telephone number ● Location data ● Online identifier, such as voucher number It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Privacy policy	This is how BTG informs people about how their personal information will be used.

4. The Data Controller

Bridging the Gap processes personal data relating to clients, volunteers, staff, trustees, referrers, donors, visitors and others, and therefore is a data controller, with the Board of Trustees as the persons responsible.

Bridging the Gap (Manchester) (BTG) is registered as a data controller with the Information Commissioner's Office (ICO) registration number ***ZA294550*** and will renew this registration as and when legally required to do so.

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.

5. Roles and Responsibilities

This policy applies to volunteers and **all staff** employed by BTG, and to supporters, Trustees and external organisations or individuals working on BTG's behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees

The Trustee Board has overall responsibility for ensuring that BTG complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring BTG's compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Trustee Board and, where relevant, report to the Board their advice and recommendations on the Charity's protection issues.

The DPO is also the first point of contact for individuals whose data BTG processes, and for the ICO.

5.3 Project Manager Responsibilities

The Project Manager acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff Responsibilities

Staff are responsible for: -

- Collecting, storing and processing any personal data in accordance with this policy
- Informing BTG of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances: -
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Collecting Personal Data

6.1 Lawfulness, Fairness and Transparency

BTG will only process personal data where it has one of six ‘lawful bases’ (legal reasons) to do so under data protection law: -

- The data needs to be processed so that BTG can fulfil a contract with the individual, or the individual has asked BTG to take specific steps before entering into a contract
- The data needs to be processed so that BTG can comply with a legal obligation

- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life

- The data needs to be processed so that BTG, as a public authority, can perform a task in the public interest, and carry out its official functions

- The data needs to be processed for the legitimate interests of BTG or a third party (provided the individual's rights and freedoms are not overridden)

- The individual has freely given clear consent.

For special categories of personal data, BTG will also meet one of the special category conditions for processing, which are set out in the GDPR and Data Protection Act 2018.

Employers must seek permission from their employees to request personal medical documents from their relevant health practitioners, as outlined in the 'Access to Medical Reports Act 1988.

When recruiting, BTG will be careful not to use information on the candidate from social media, unless there is a clear reason to do so. In this latter case BTG would allow the candidate to make representations in relation to the content.

6.2 Limitation, Minimisation and Accuracy

BTG will only collect personal data for specified, explicit and legitimate reasons. BTG will explain these reasons to the individuals when it first collects their data.

If BTG wants to use personal data for reasons other than those given when it was first obtained, it will inform the individuals concerned before it does so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the ICO.

7. Sharing Personal Data

BTG will not normally share personal data with anyone else, but may do so where:

- There is an issue with a client that puts the safety of BTG's staff and volunteers at risk

- BTG needs to liaise with other agencies. BTG will seek consent as necessary before doing this

- BTG's referral agencies, suppliers or contractors need data to enable the Charity to provide services to its clients – for example, community facilitators.

  When doing this, BTG will: -

- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

BTG will also share personal data with law enforcement and government bodies where we are legally required to do so, including for: -

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

BTG may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our clients, volunteers or staff.

8. Subject Access Requests and Other Rights of Individuals

8.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that BTG holds about them. This includes: -

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email or to the DPO. They should include: -

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

8.2 Responding to Subject Access Requests

When responding to requests, BTG: -

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual BTG will comply within 3 months of receipt of the request, where a request is complex or numerous. BTG will inform the individual of this within one month, and explain why the extension is necessary.

BTG will not disclose information if it: -

- Might cause serious harm to the physical or mental health of the client or another individual
- Would reveal that the client is at risk of abuse, where the disclosure of that information would not be in the client's best interests
- Is contained in court documentation
- Is given to a court in proceedings concerning the client.

If the request is unfounded or excessive, BTG may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When BTG refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

8.3 Recording Subject Access Requests

A record will be kept of all Subject Access Requests (SAR) and logged on the SAR database. This SAR folder and database will be securely stored on site.

A file is to be created for each subject access request and in it should be the following information:-

- Copies of the correspondence between BTG and the data subject, and between BTG and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject
- A record of the decisions and how BTG came to those decisions

- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

The file will be kept for one year and then securely destroyed.

When the request has been completed, the record of the request will be closed in the database.

8.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when BTG are collecting their data about how it uses and processes this information (see section 7), individuals also have the right to: -

- Withdraw their consent to processing at any time
- Ask BTG to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision-making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Photographs and Videos

As part of BTG's activities, it may take photographs and record images of individuals accessing our services or contributing to the facilitation of services.

BTG will obtain written consent for photographs and videos to be taken for communication, marketing and promotional materials. BTG will clearly explain how the photograph and/or video could be used to the individual. In the instance of children consents will be sought from their parents/carers

Uses may include: -

- On community notice boards and in BTG's newsletters, evaluations and annual reports, etc. Outside of BTG by external agencies such as photographers, newspapers, campaigns, donor news feed

- Online on BTG's websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, BTG will delete the photograph or video and not distribute it further.

10. Data Protection by Design and Default

BTG will put measures in place to show that it has integrated data protection into all of its data processing activities, including: -

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where BTG's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; BTG will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure BTGis compliant

- Maintaining records of BTG's processing activities, including: -

    - For the benefit of data subjects, making available the name and contact details of DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

    - For all personal data that BTG holds, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

11. Data Security and Storage of Records

BTG will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular: -

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data will be kept under lock and key when not in use
- Papers containing confidential personal data will not be left on office desks, on tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff will sign it in and out from the office
- Passwords of at least 8 characters long and/or 4 digit pin numbers will be used to access computers, laptops and other electronic devices
- Staff, and Trustees who store personal information on their personal devices will be expected to follow the same security procedures as for BTG-owned equipment (see our IT Acceptable Use Policy)
- Where BTG needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

12. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out-of-date will also be disposed of securely, where BTG cannot or does not need to rectify or update it.

For example, BTG will shred paper-based records, and overwrite or delete electronic files. BTG may also use a third party to safely dispose of records on the Charity's behalf. If BTG does so, then it will require the third party to provide sufficient guarantees that it complies with data protection law.

13. Personal data breaches

BTG will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, BTG will follow the procedure set out in Appendix 1.

When appropriate, BTG will report the data breach to the ICO within 72 hours. Such breaches in a Charity context may include, but are not limited to: -

- A non-anonymised dataset being published on BTG's website, which shows the clients eligible for benefits

- Safeguarding information being made available to an unauthorised person

- The theft of a BTG laptop or device containing non-encrypted personal data about clients

14. Training

All staff and Trustees are provided with protecting information training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or BTG's processes make it necessary.

15. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when legislation changes are made that affect BTG's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the Board of Trustees.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- Data protection breaches could be caused by a number of factors. Some examples are: -
    - Loss or theft of client, volunteer, staff or Trustee data and/ or equipment on which data is stored
    - The sharing of system passwords
    - Inappropriate access controls allowing unauthorised use
    - Equipment Failure
    - Human Error
    - Unforeseen circumstances such as fire or flood
    - Hacking
    - 'Blagging' offences where information is obtained by deception.
- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO)
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully: -
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people.
- The DPO will alert the chair of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure.)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:-

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the designated, protected folder on a laptop.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out: -

    - A description of the nature of the personal data breach including, where possible: -
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out: -

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals. For example: the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the designated, protected folder on a laptop.

Review and Evaluation

The DPO and Project Manager will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Once the initial aftermath of the breach is over, the DPO and Project Manager should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Trustee Board meeting for discussion. If there is the perception that this could be a continuing risk, the Trust's risk register is to be updated accordingly and an action plan must be drawn up to address the risk. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Actions to Minimise the Impact of Data Breaches

BTG will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. BTG will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records):-

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public. If it has, BTG will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.