Bridging the Gap (Manchester)
Confidentiality Policy

Registration number/charity number: 1170952

This policy and guidance will be reviewed at least every 18 months or sooner if there are any changes in the related legislation or when an incident dictates. This will ensure that this document is current and fit for purpose.

This policy should be read in conjunction with the following Bridging the Gap's policies and procedures: -

- Social Media Usage Policy & Procedure
- Safeguarding Policy & Procedure
- Whistleblowing Policy & Procedure

Date reviewed: 23/01/2026
Reviewed by: Michelle McHale
Next review due: 23/01/2028

Contents:

1. Purpose and Principles:

Bridging the Gap (BTG) is committed to maintaining the highest standards of confidentiality in all aspects of its work. This includes information relating to employees, volunteers, service users, and prospective service users.

The purpose of this policy is to:

- Set out how BTG manages, stores, and shares personal information.
- Protect the rights, dignity, and safety of all individuals who engage with BTG.
- Clarify circumstances where confidentiality may need to be broken.
- Ensure compliance with UK GDPR and the Data Protection Act 2018.

BTG aims to provide a confidential service. All staff and volunteers must treat with confidence any information obtained about individuals using BTG's services. "Treating with confidence" means not disclosing information to others without the individual's explicit permission, unless an exception applies under this policy.

Safeguarding always takes precedence over confidentiality.

2. Internal Confidentiality:

Confidentiality exists between service users, volunteers and staff however,

- Information may be shared internally on a **strict need-to-know basis** to ensure safe and effective support.
- Service users will be informed that relevant information may be shared within the team.
- Information may be shared with referral agencies unless a service user requests otherwise and there is a valid reason to restrict sharing.

3. Case Files and Client Data:

BTG processes personal data in accordance with **UK GDPR** and the **Data Protection Act 2018.**

Data Storage

- Physical records are stored in a **locked cabinet within a locked office.**
- Digital referral voucher information is stored on a **secure, two factor protected database** accessible only to authorised personnel.
- All IT equipment is password protected

Retention

- Personal data will be retained for **no longer than two years,** unless a longer period is required for safeguarding, legal or operational reasons.
- BTG uses secure destruction methods for all expired records.

Access to information (Data Subject Rights)

Any service user, employee, or volunteer may request access to the information BTG holds about them

Requests should be submitted to the Operational Project Manager. BTG will respond within **30 Days**, in line with UK GDPR.

4. Information Sharing:

To provide effective support, BTG may need to share information with other professionals, or organisations such as referral agencies or partner services.

- BTG will seek **informed Consent** (written or verbal) where possible.
- Consent will be recorded appropriately
- Consent **is not** required where there is a safeguarding concern, legal obligation, or risk of serious harm.
- Information will only be shared on a **need-to-know basis** and in line with UK GDPR and the Data Protection Act 2018.
- When information is shared without consent, the rationale will be documented and reported to the Project Manager or Safeguarding Lead.

5. Social Media:

- Personal information about service users must **never** be shared on public social media platforms.
- Photographs or videos of individuals may only be taken and shared with express written consent.
- Staff and volunteers must maintain the highest level of confidentiality when using social media.
- All social media platforms must be password protected and only used by those authorised to use.

6. Exceptional Circumstances:

Confidentiality may be broken when necessary to protect an individual or comply with the law.

Exceptional circumstances include:

Safeguarding risks:

- Serious risk of harm to self or others
- Suspected abuse or neglect
- Concerns relating to forced marriage or female genital mutilation
- Situations where an individual lacks mental capacity and sharing is in their best interest.

Legal obligations:

- Court appearances requiring disclosure
- Police and Local Authority safeguarding investigations.
- Information relating to terrorism

Criminal activity:

- Evidence of drug dealing within BTG's services
- Other criminal behaviour poses risk to individuals or the organisation.

Immediate risk to life:

- Urgent medical emergencies requiring disclosure to emergency services.

Safeguarding always overrides confidentiality.

7. Procedure for Breaking Confidentiality:

If a staff member or volunteer believes confidentiality must be broken:

1. Report the concern immediately to the **Operational Project Manager** or, in their absence, the **Trustee Safeguarding Lead.**
2. Provide clear evidence or rationale for the disclosure.
3. The decision to break confidentiality will be made by the safeguarding Lead or Operational Project Manager.
4. Any unauthorised breach of confidentiality may result in disciplinary action.

8. Police and Local Authority Safeguarding Teams:

All requests for information from the police or Local Authority Safeguarding Teams must be directed to:

- The **Operational Project Manager,** or
- In their absence, the **Chair of Trustees and Safeguarding Lead.**

BTG has a duty of care to all service users, volunteers, visitors, and paid staff.

9. Personal Information:

Personal details - including their home address, phone numbers, email addresses, and social media accounts - must not be shared without the individual's explicit permission.

The only exception is where there is reasonable cause to believe a child or vulnerable adult is at risk of significant harm.

10. Confidentiality Training

All staff and volunteers receive confidentiality training during their induction. This training covers BTG's confidentiality expectations, data protection responsibilities, safeguarding requirements, and procedures for information sharing.

Refresher training is provided annually or whenever policies or legislation change. Staff and volunteers must demonstrate an understanding of their responsibilities before handling personal information.

Breaches of confidentiality may result in disciplinary action or termination of role.

11. Appointed Safeguarding Personnel:

Trustee Safeguarding Lead:

- Michelle McHale BEM (Chair)
  Michellemchale@manchestersouthcentral.foodbank.org.uk

Deputy Safeguarding Officers:

- Operational Project Managers -
  Projectmanager@manchestersouthcentral.foodbank.org.uk

- Assistant Project Manager
  Volunteers@manchestersouthcentral.foodbank.org.uk