Bridge Group
research
action
equality

Data Security and Confidentiality Policy

Current version: February 2023

Introduction

1. This policy sets out the protocols for keeping confidential information secure.

2. All Bridge Group colleagues (including employees, interns, Associate Researchers, Fellows and other contractors) engaged to undertake Bridge Group research must adhere to this policy.

3. This policy is to be read in conjunction with the BG Guide to GDPR, IT Use Policy and website privacy policy.

Confidential Information

4. **Confidential Information** in this policy is defined as:

   4.1. any Personal Data[1] processed[2] for research or other purposes. This will most commonly take the form of names and contact details of research participants; research data

[1] 'Personal Data' means any information relating to an identified or identifiable person ('data subject') as set out in the UK Data Protection Act 2018. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more features specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[2] Processing means doing any of the following to data: collecting; recording; organising; structuring; storing; adapting; altering; retrieving; consulting; using; disclosing; transmitting; disseminating; making available; aligning; combining; restricting; erasing; and destroying.

that features identifiable characteristics (e.g. names, addresses, unique job titles or role descriptions etc.) or might cause identification of an individual when taken as a whole; the demographic / contact details of Bridge Group colleagues and trustees; and the contact details of clients, other stakeholders and newsletter subscribers.

4.2. any other forms of research data held or processed on behalf of a client / third-party or for internal research (e.g. anonymised data that does not contain any Personal Data but is still confidential and /or may be sensitive when linked to a client or viewed as a whole). This includes purchased research data (from UCAS, HESA etc.);

4.3. any information held that is marked confidential, or is reasonably understood to be confidential, whether received from a client / third party, or produced internally. This might include commercially sensitive or protected materials, images or video files obtained in the course of research or embargoed documents shared prior to publication (which will cease to be confidential after publishing).

5. Confidential Information must be kept in a secure, password protected location at all times (see point 23) and must not be shared outside the organisation. The only exceptions are where:

5.1. The owner / provider of the Confidential Information (and/or data subject in the case of Personal Data) agrees, in writing, that it may be shared.

5.2. The Confidential Information becomes freely available in the public domain due to a planned release, or through other means not relating to a breach of confidentiality by a Bridge Group employee, intern or contractor, or a third party.

5.3. The employee, intern or contractor had no reasonable way to know that the Confidential Information was confidential prior to sharing (e.g. it was not marked confidential or obviously confidential by its nature and was openly shared).

5.4. An employee, intern or contractor is required to share the Confidential Information by law, regulation or reasonable request by the government or judiciary.

6. Some forms of Confidential Information, particularly Personal Data and other research data, will require additional protections (see Data Security section below) when storing, processing or transferring.

7. Some clients may set out additional stipulations regarding confidentiality and data security as part of their contract with the Bridge Group, or will request the Bridge Group signs a separate confidentiality, data security and/or data sharing agreement. Bridge Group colleagues must take these additional requirements into consideration when processing Confidential Information. Where any conflict arises between this policy and the stipulations of the client, this should be communicated to the client so an agreed approach can be established. The requirements of this policy should always be adhered to, even where the stipulations of the client are less rigorous or detailed.

8. Upon leaving the organisation, an employee, intern or contractor of the Bridge Group must draw up a plan for the secure transfer and / or removal of all files from devices containing Confidential Information (see point 28 below). This plan must be reviewed by the Chief Executive and, where relevant, a Senior Researcher and executed and checked prior to that individual's departure. All access to Bridge Group e-mail and shared drives should be removed within twenty-four hours of the individual's departure.

Data Security

9. Confidential Information classified as "data" (e.g. Personal Data and any other data obtained from clients, research participants or third parties) must be processed securely, accurately, and in accordance with the UK Data Protection Act 2018 and General Data Protection Regulation (please see the Bridge Group Guide to GDPR).

10. The following clauses refer to "data security", but the protocols given may be used to secure any form of information deemed confidential or sensitive.

11. Any questions regarding data handling and security should be directed towards the Chief Executive and the appointed data security officer(s) – usually the Head of Operations. The Chief Executive should also be informed in the event of a breach (as detailed in point 30).

12. **Data minimisation**: The Bridge Group adheres to the principle of data minimisation: we limit the identifiable data we ask for to the minimum needed for our purposes and, wherever possible, only handle anonymised data.

13. **Anonymisation:** Colleagues should always seek to anonymise all data held as far as possible. Immediately identifying data (names, e-mail addresses, specific job titles etc.) should always be excluded from any data files received from clients, and only held in our own files if absolutely necessary (e.g. for sending updates to participants / clients or newsletters to supporters etc).

    13.1. Data collected through interviews should not include participant names or contact details (though these may be held separately for communication purposes) in the transcripts and associated notes, and any other immediately identifying data should ideally be redacted or pseudonymised before storage.

    13.2. Pseudonyms (i.e., unique ID numbers) may be used to replace personal/identifiable information where we need to be able to trace data back to an original source, but the key must be kept secure and password protected at all times (and not shared with us at all if the data is supplied pre-pseudonymised by a client).

    13.3. Data that is pseudonymised, or only partially anonymised (i.e. still contains characteristics that, in combination, might be used to identify an individual), is still considered Personal Data under GDPR, and we must therefore follow the guidelines found in the BG Guide to GDPR.

14. **Usage:** all data (including pseudonymised and anonymised data) held by the Bridge Group must only be used to carry out the permitted purpose as specified in any associated contract, data sharing agreement, survey privacy notice, interview consent form or the website privacy policy.

    14.1. Attempting to identify individuals within data pre-pseudonymised or anonymised by a client or other third party is in violation of this policy and most other typical data sharing agreements, and is a disciplinary offence; if the identity of any individual is discovered inadvertently, this information is not to be used, but should be reported immediately to the project lead. Colleagues must alert the CEO / project lead if they know individual(s) who may appear in the data set so the analysis can be assigned to someone else.

15. **Sharing and access:** all data should be kept confidential and should never be shared outside of the project specification, or in the case of Personal Data collected for non-research purposes (e.g. newsletter subscription) outside the specifications found in the website privacy policy.

    15.1. Only authorised Bridge Group employees (and if agreed in writing by the CEO and client, fully vetted Associate Researchers and Interns) may be granted access to confidential client data.

16. **Reporting:** Individuals should not be identifiable in any report produced at the end of a project (e.g. by the position they hold in an organisation, by their specific demographic characteristics when there are small numbers meeting the same combination, or by their experiences) nor in any related summaries, press releases or other media. In general, data should be supressed where numbers are less than five (dependent on dataset size).

17. **Rights of data subjects:** these apply to all subjects on whom we hold Personal Data: the right to erasure, the right to access by the data subjects, the right to rectification, the right to restrict processing, the right to object to processing. See the BG Guide to GDPR for more information. The website privacy policy, or for surveys we undertake, template privacy notice, give further details of how data subjects can contact The Bridge Group to make changes, withdraw data or consent, etc.

    17.1. It is important to be clear with data subjects how their data is being captured (i.e., if using audio recording, obtain consent), how data will be used, and their right to withdraw. Research participants must be provided with a named Bridge Group contact in case they wish to withdraw their consent. Other data subjects should be referred to the 'controlling your personal information' section of the privacy policy.

18. **Transfer:** When receiving research data from an outside party (e.g. a client), a data sharing agreement should be signed before transfer, and the most secure method available should be used to transfer the data. Wherever possible, individual data files should be password protected (see point 26). If files are received without password-protection, the party sending the data should be informed that the

data cannot be processed and should be asked to transfer the file(s) again in a password-protected format, with the original message then deleted. Bridge Group approved data transfer processes include:

18.1. Direct, password protected access to a client-owned storage drive (if the client is happy to grant this). The files, if possible, should remain in this drive and not be downloaded to further strengthen security.

18.2. Transfer via a secure, encrypted file sharing service or app (Bridge Group recommends MailBigFile – see IT Use policy).

18.3. In person transfer on an encrypted USB stick, with data downloaded to a secure hard drive and the stick subsequently formatted to delete all data and destroyed.

18.4. Encrypted e-mail (small datasets only) with data downloaded to a secure drive. Gmail users can employ the confidential setting, which will prevent copying and forwarding and cause the e-mail to expire after a specified time.

18.5. In person access – for extremely sensitive data, clients may request we only work on the data at their offices / on their systems, with no raw data transferred to ours.

19. **Secure Environments:** The Bridge Group shall store data in a secure environment in compliance with the charity's Cyber Essentials certification. Access shall be limited to the fewest number of colleagues needed to complete the purpose of the assignment.

20. Data must be categorised and labelled as CONFIDENTIAL HIGH / MED / LOW according to type:

20.1. Low sensitivity (fully anonymised data and low-risk documents). This can be stored in relevant Shared Google Drive folder (with no external access).

20.2. Medium sensitivity (contains pseudonymised or partially anonymised Personal Data i.e. with immediately identifying data removed and no Special Category data) This can be stored in a researcher's personal Google Drive with access granted only to those who need it for analysis.

20.3. High sensitivity (contains identifying Personal Data, Special Category data or data highlighted as especially sensitive –

e.g. salary info). This should be stored only on the hard drive of the researcher who will be analysing. Any sharing with colleagues must only be done if strictly necessary and via an approved transfer method (e.g. encrypted e-mail with no forwarding allowed and expiry set to 1 hour).

21. Colleagues should minimise the number of devices from which the data can be accessed. Personal mobile phones should not be used to access or store data (this includes opening any data files attached to e-mails) unless the mobile is fully encrypted, has anti-virus software running and the access has been specifically authorised by a line manager or project lead and/or client.

22. Only employees shall be granted full access to Bridge Group systems (e.g. Google Workspace). Associate Researchers and Interns may be granted a Bridge Group e-mail address if working with us regularly / long term, but must not be given access to the Shared Drive as a whole. They may be granted access to specific folders that contain only data needed to do their job. This should be revoked as soon as they have completed their assignment.

23. All colleagues must ensure their individual laptops, mobile phones (and any removable memory cards within them), or other device used to access or store data are fully secure by implementing the following measures as a minimum:

    23.1. Restricting access to authorised users by requiring logon to any relevant workstation or portable device using a unique user ID and complex password (see point 26) or other authentication mechanism which provides equal or greater security. This applies to all computers, storage systems and portable devices, i.e., any USB drives, back-ups on hard drives, etc.

    23.2. Only storing data where specifically authorised and where the device is given the following protections:

        23.2.1. A unique username and password (laptops) or pattern / pin / biometric data (mobiles) to access.

        23.2.2. Data encryption with a key length of at least 128 bits (e.g. BitLocker for Windows, FileVault for Mac or appropriate built-in or downloaded encryption for mobile phones).

23.2.3. Manual locking of the device whenever it is left unattended and automatic locking after a period of inactivity, if this feature is available. Maximum period of inactivity is 15 minutes.

23.3. Encrypting any photography and video files, and where this is not possible (often photography / video devices do not contain the ability to encrypt images stored on the device), transferring files as soon as practical to a secure location, with the files securely deleted from the device / memory card. This will prevent unauthorised access if the device or a memory card is lost or stolen. The transfer process, even if an encrypted device such as a phone / tablet is used, should also be secure (i.e., must avoid automatic upload to a remote cloud service or social network, avoid transfer as an unencrypted email attachment etc.).

23.4. Switching on any pre-installed security app on mobile phones authorised to access secure data or downloading and enabling a security app if a pre-installed app is not available. The theft protection / locate my device feature should also be enabled.

23.5. Ensuring data is never entered into web-enabled or online software (such as translation or online editing / file conversion software) unless its security can be fully guaranteed.

23.6. Turning off any automatic backups (e.g. to the cloud or an external hard drive) unless the data files are backed up to a drive that is equally secure.

24. **Protecting hard copy data**: This includes things such as printouts of confidential documents, notes which contain identifying information, non-digital recordings and data storage which cannot be encrypted or password protected (i.e., mp3 recorders, CDs). Physical copies of data should be kept to a minimum (i.e. only printing if strictly necessary). As far as possible, these physical items, where unattended, must be protected by storing them in locked filing cabinets or hiding them from view (i.e., if travelling, by keeping them in a closed bag or the glove compartment of a car). Only authorised individuals should have access to any area where confidential physical materials are kept.

25. **Protecting Individual Files**: Wherever possible, individual files containing sensitive data are to be protected via password (see point

26). It is possible to do this in many programs using built-in encryption (PDF, PowerPoint, Excel, etc.) but specialist software can also be used (the Bridge Group recommends 7Zip).

26. Passwords: Passwords should be lengthy and strong / complex. They should have at least 8 characters (12 or more is preferable) and feature a combination of upper- and lower-case letters with numbers and special characters. No personal information should be included. A good way to generate strong and memorable passwords is to use the three random words method.

    26.1. Passwords should be changed regularly (at least once every three months), and different passwords used for different purposes (i.e., never use the same password for files, email account, and computer).

    26.2. A password should never be shared with anyone who is not authorised to access the data it protects.

    26.3. It is good practice to avoid writing down passwords, but if difficult to remember, they may be stored somewhere securely, such as a password safe app.

    26.4. When text messages, emails, etc. containing passwords are no longer required, they must be securely deleted.

27. Software:

    27.1. New software: Colleagues should follow the Bridge Group IT policy at all times, and only download software to their Bridge Group device that is authorised. Other software may be agreed at a line manager's discretion provided it comes from a reputable source, will not pose a threat to data security and is essential for work. No software for file transfer or data storage should be used other than that authorised. If in any doubt, employees should contact the Finance and Operations Officer for guidance.

    27.2. Laptop security: Anti-virus software and a VPN must be installed and set to run constantly on all employee laptops (see the Bridge Group IT policy).

        27.2.1. Operating system and application updates should be installed as soon as available. While most operating systems and applications will update automatically, where they do not, colleagues should update within 14 days of notification.

27.2.2. Project leads should check the above provisions are also in place (as a minimum) when sharing data with Associate Researchers and Interns, who may be using their own laptops.

27.3. E-mail: Any email concerning work must be sent via an employee's (or where they have one, Associate or Intern's) Bridge Group Gmail account. Google accounts have a security check-up option and it is recommended that this is run. Wherever possible, a two-step verification option should be enabled. Users should be logged out every evening.

27.4. Secure deletion software: This should be used when removing data from the hard drive (see point 28 below). The Bridge Group recommends Eraser, or Permanent Eraser for Mac.

27.5. Printers: only print when strictly necessary, and ensure the printer is on a closed, secured (password protected) network before printing.

27.6. File sharing within the Bridge Group: See point 20. Files must categorised according to sensitivity and stored and shared accordingly. Always password protect before sharing, and share the password separately from the file (via text or encrypted e-mail with expiry set to one hour).

27.7. File sharing outside the Bridge Group: password protect, only use one of the preferred transfer methods outlined in point 18, and verify receipt.

28. Destruction of data and devices:

28.1. Electronic data: This includes any files on a laptop, such as an Excel spreadsheet or SPSS file. Any files containing Personal or sensitive data should be password protected and when they are no longer required, should be securely deleted as soon as possible. Placing a file in the 'recycle bin' and then deleting from there ('emptying the recycle bin') is not sufficient for it to be removed from a computer. Using secure deletion software (as mentioned in point 28.5.1) ensures that a file has been properly removed from a laptop and cannot be recovered.

28.1.1. Data will usually be downloaded from an email or from a file transfer system. It is important to ensure that the email containing the file is deleted and the file is also deleted from any downloads folder.

28.1.2. It is recommended that regular deletions / clean ups of the download folder and recycle bins are scheduled. Download files can also be set to download automatically to specific, secure folders.

28.1.3. Any backups of the data should be deleted at the same time as the original data.

28.1.4. If files containing data are placed onto portable / external storage devices (USB sticks, external hard drives, etc.) then once the files are no longer needed, they should be deleted using secure deletion software and / or device formatting.

28.1.5. If viewing data on a phone and / or tablet, be aware that this information will need to be deleted from the device once no longer needed, and the device formatted before it is sold / disposed of.

28.2. Physical documents: When the documents are no longer needed, they should be destroyed. In the case of paper and items like CDs, these should be shredded either through a confidential service or using a cross shredder (cross-cut shredders cut both vertically and horizontally, further reducing the risk that paper pieces can be ‘puzzled’ back together).

28.3. Survey data: any survey data stored in an online survey service (the Bridge Group uses TypeForm) once a project has finished must be deleted in full as soon as practical. Survey applications will be checked once every six months by the Senior Researcher (qualitative) and her team to ensure this has occurred.

28.4. Timing of data deletion: Where there are specific instructions on the length of time that we will hold data within data sharing agreements, these must be adhered to. In all other cases, after a project has ended (final presentations made, report in final format etc.), files with raw data must be securely erased as soon as possible, ideally within 14 days. (N.B. some contracts may also require erasure of outputs – this should be checked and undertaken where applicable). Bridge Group shared files will be checked every six months to ensure no unnecessary data remains in project folders and colleagues will be reminded to do the same with their personal files.

28.5. Destruction of devices: When no longer using a device for work purposes, i.e., after a laptop or phone upgrade, all data should be removed.

28.5.1. Laptop computers: Secure deletion software should be used (see the IT Use Policy for suggestions) to ensure all data has been removed securely, or ideally, a format / restore to factory settings function should be run.

28.5.2. Mobile phones and tablets have a factory reset option that should delete all data on the phone. Where additional memory cards are used or data is saved to the SIM card, these should be formatted or taken out and physically destroyed.

29. **Employee awareness:** Colleagues should receive a full briefing on data security, in line with this policy, upon joining / contracting with The Bridge Group. Once per year, to coincide with the annual renewal of the Bridge Group Cyber Essentials certification, employees will also receive a refresher briefing, with any amendments to this policy clearly communicated in the interim.

29.1. Any colleague who identifies a possible data security risk should report it immediately to the Chief Executive, who will work with colleagues to correct the issue or find a suitable mitigation as soon as possible.

30. **Data breach:** This is where Personal Data is shared and / or accessed by persons outside of the project team and charity without authorisation, or where data becomes unaccounted for.

30.1. Breaches may include, but not be limited to:

30.1.1. Malware attacks that allow access to hackers
30.1.2. Ransomware attacks that demand payment for release of files
30.1.3. Releasing (through in person or postal transfer or accidental loss / theft) physical or digital hard drive copies of data

30.1.4. E-mailing or transferring data to an unauthorised person / organisation (including copying unauthorised parties into e-mails to authorised ones)

30.1.5. Copying recipients of newsletters and similar e-mails in the To: or Cc: line, rather than Bcc:.

30.1.6. Entering data into an unsecure online application (including online translation, editing or file conversion programs or AI software)

30.1.7. Posting data / information (partially or in full) on social media such as LinkedIn, Facebook, Twitter etc. or on a forum or website (ours or any third party's)

30.1.8. Allowing data to be shared in visual format (e.g. including sensitive data in the background of a photo posted online)

30.1.9. Leaving data on screen for someone to view

30.2. In the event of a data breach or potential breach, this must be communicated to the Chief Executive as soon as possible (or Head of Operations in their absence).

30.3. The Chief Executive will assess the situation and initiate an appropriate plan working with other colleagues and external organisations as required. Clients affected by the breach should be informed as soon as possible, and always within 24 hours of the CEO receiving notification.

30.4. Common courses of action will include but are not limited to: recall of communications, contacting those affected by the breach, changing passwords, freezing or taking offline certain accounts, engaging specialists to assist etc.

30.5. If a data breach is sufficiently serious, the BG's insurers (who can provide assistance in breach impact mitigation), the Information Commissioner's Office and potentially the Charity Commission may need to be informed. Further details of what constitutes a serious breach and be found on the ICO and Charity Commission websites.

30.6. Other data security concerns (including virus alerts and suspected phishing) should be reported to the Finance and Operations Officer and Head of Operations within 24 hours.

31. **Further information**: further information on physical, online and data security can be found through the government cyber aware and get safe online website, while the Information Commissioner's Office advice for charities is available here.