Bridge Group
research
action
equality

Data Security and Confidentiality Policy

1. This policy sets out the protocols for how qualitative and quantitative data will be processed securely, accurately, and in accordance with data protection principles.

2. All employees at the Bridge Group and sub-contractors (e.g., Bridge Group Fellows engaged in undertaking Bridge Group research) must adhere to this policy.

3. This policy is to be read in conjunction with the privacy policy available here.

4. Any questions regarding data handling and security or in the event of a breach (as detailed in point 23) should be directed towards the Chief Executive and the appointed data security officer(s).

5. 'Personal data' means any information relating to an identified or identifiable person ('data subject'); 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.

6. 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.

7. We adhere 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.

8. Anonymisation: data that are processed by The Bridge Group are not usually personal and identifiable, but where they are such data need to be pseudonymised or fully anonymised.

    8.1. Pseudonymised data comprises the removal of personal/identifiable information often with artificial identifiers (i.e., unique ID numbers) or pseudonyms. Such artificial identifiers mean that a key and/or a group of people can be used to identify individuals within the data, therefore pseudonymised data still need to be treated with care.

    8.2. Truly anonymising personal data is best where possible and requires the complete removal of all personally identifiable information with the deletion / destruction of the original identifiable data. Note that the process of anonymisation is still processing of personal data. If we are only accessing an anonymised database, with which there is no other means of identifying the individuals (either by the combination of the data collected or by combining the data with other information held, or accessible, by us) then we are not processing personal data.

9. Usage: Personal data we hold must be treated confidentially, and only used to carry out the permitted purpose as specified in a data sharing contract agreed in advance with a client or a policy relating to in-house research. Using the data to identify individuals is in violation of typical data sharing agreements; if the identity of any employee is discovered inadvertently, this information is not to be used, but should be reported immediately to the project lead. Data are not to be shared outside of the project specification.

10. Reporting: Individuals should also not be identifiable in the reporting (e.g. by the position they hold in an organisation, by their specific demographic characteristics when there are small numbers meeting the same combination, by their experiences). Permission must be sought from participants to use named quotes in reporting, presentations etc.

11. Rights of data subjects: These apply to all subjects on whom we hold 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 privacy policy for details of how data subjects can contact The Bridge Group to make changes, withdraw data, etc.

    11.1. Be clear with participants about how their data are being captured (i.e., if using audio recording, obtain consent), how data will be used and their rights to withdraw. Provide a named individual and contact details should they decide to withdraw, or refer participants to the 'controlling your personal information' section of the privacy policy.

12. Photography and video: Often photography / video devices do not contain the ability to encrypt images stored on the device. This may risk unauthorised access if the device or a memory card is lost or stolen. In this instance, the images / video should be transferred as soon as it is practical to a secure location, and securely deleted from the device / memory card. This 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).

13. Secure environments: Data are to be stored in secure environments with access limited to the fewest number of staff needed to complete the purpose of the research as set out in the project specification. This includes but is not limited to the following:

    13.1. Access to the data is restricted to authorised users by requiring log-on to any relevant workstation or portable device using a unique user ID and appropriate password or other authentication mechanisms which provide equal or greater security

    13.2. Data shall not be stored on any portable devices or media unless specifically authorised and shall be given the following protections:

        13.2.1. Encrypt the data with a key length of at least 128 bits. This is standard for software such as Microsoft Office (Word, PowerPoint, etc.) but for other types of files (i.e., PDFs) or other password protection / encryption software you may need to choose a setting such as AES128.

        13.2.2. Control access to devices with a unique user ID and password.

        13.2.3. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

    13.3. Protect data in a manner that prevents unauthorised persons from retrieving the data by means of computer, remote terminal or other means.

13.4. Any paper records must be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

14. Files containing sensitive data are to be protected via password. It is possible to do this for all matter of programmes using built-in encryption - PDF, PowerPoint, Excel, etc. – ask if you need assistance. Make sure your programmes are up to date. Additional free software such as 7zip can be used to password protect files.

15. Devices on which Bridge Group business containing sensitive data is accessed are to be protected via password. This applies to all computers, storage systems and portable devices, i.e., any USB drives, back-ups on hard drives, etc.

16. Mobile phones: Most mobile phones come with a pre-installed security app and this should be enabled, or a security app downloaded and enabled. The theft protection / locate my device feature should also be enabled. Similar to laptops, etc., mobile phones need to require a log-in (pattern or pin number) to unlock.

17. Passwords: Good practice guidance in passwords is to make passwords lengthy and strong / complex. This can be achieved by having passwords that are at least 8 characters long (12 should really be the minimum) and for the characters to be a combination of upper- and lower-case letters with numbers. No personal information should be included in passwords. A good way to generate strong and memorable passwords is to use the three random words method.

17.1. It is good practice to regularly change your passwords, and to use multiple passwords (i.e., do not use the same password for your file, email account, and computer).

17.2. It is good practice to avoid writing down passwords but if you need to keep a note of them somewhere, this needs to be kept secure or stored in an app such as password safe.

17.3. When text messages, emails, etc., containing passwords are no longer required, please ensure they are deleted.

18. Software:

18.1. Personal/work laptop security: Install virus software and ensure you regularly check for / install updates and scan regularly. Free software includes Avast and Sophos.

18.2. E-mail: Any email concerning work must be done via the Bridge Group Gmail account. Google accounts have a security check-up option and it is recommended that this is run. It is highly recommended to enable the two-step verification option for log-ins after a specific time period / on new devices.

18.3. Secure deletion software: This is for when you are finished using files that are confidential / contain personal information – you can delete them securely off of your hard drive (putting them in the 'trash' will not erase them completely). Free software includes Eraser, or Permanent Eraser for Mac.

18.4. File sharing within the Bridge Group: When sending files with sensitive content to colleagues, password protect files, send the files in an email and send the password separately in a text message or separate email (not using the word password). When using Google Docs, double check that the sharing / viewing settings are restricted to specific people or those with a Bridge Group email.

18.5. File sharing outside of the Bridge Group: The protocol to follow when colleagues outside the organisation need to send data is:

18.5.1. Ensure a data sharing agreement is in place
18.5.2. Have them password-protect all data
18.5.3. Have them send the password in a text message
18.5.4. Have them use this link to upload the data
18.5.5. A secure download link will be sent to the data security officer, who will send you a download link to access the site and download
18.5.6. Upon downloading and checking that the file is accessible, confirm safe receipt and access to colleagues

19. In the event that you receive data that are not password-protected, inform the party sending the data that we cannot process these data, ask that they send it again in a password-protected format and delete the original message.

20. Regularly clear your browsing history and securely empty your downloads file (or set files to download automatically to specific files).

21. How long before deleting data: There are specific instructions on the length of time that we will hold data within data sharing agreements and we must adhere to these. After the project has come to an end (defined as past the final presentations, report in final format), securely erase files with raw data, leaving only outputs (NB Refer to contracts as some contracts may also require erasure of outputs).

22. Destruction of data and devices:

22.1. Electronic data: This includes any files on a laptop, such as an Excel spreadsheet. Any files containing personal data should be password protected and when they are no longer required need to be securely deleted. Often placing a file in the 'recycle bin' and then deleting from there ('emptying the recycle bin') are not sufficient for the file to be removed from your computer. Using secure deletion software (as mentioned in point 18.3) ensures that a file has been properly removed from your laptop and cannot be recovered.

22.1.1. In receiving a file containing personal data, you will most likely have downloaded the file from an email or from the file transfer system. You therefore need to ensure that the email containing the file is deleted and the file is also deleted from your downloads folder.

22.1.2. It is recommended that where possible you set up regular deletions / clean ups of your download folder and recycle bins.

22.1.3. If you are placing files containing personal data onto portable / external storage devices, i.e., USB sticks, external hard drives, etc., then once you no longer need the files delete the files using secure deletion software and / or format the device.

22.1.4. If you are viewing confidential documents or those that contain personal data on your phone and / or tablet, be aware that you will need to delete the files from your device and that in the future you may need to format the device.

22.2. Physical documents: This includes things such as: printouts of confidential documents, notes which contain personally identifying information, non-digital recordings and data storage which cannot be encrypted or password protected (i.e., mp3 recorders, CDs).

22.2.1. As much as possible, these physical items must be protected, for example, do not leave documents unattended. If unattended, items need to be stored in locked filing cabinets and / or hidden from view (i.e., if travelling, keep in glove compartment of car).

22.2.2. 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).

22.3. Destruction of devices: When you are no longer using a device for work purposes, i.e., when you get a phone upgrade, you need to ensure that nothing confidential or containing personal data is left on the device.

22.3.1. 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, format these or take them out and physically destroy them.

22.3.2. Laptop computers: Use secure deletion software to ensure all data has been removed securely, or ideally, run a format / restore to factory settings function.

23. Data breach: This is where personal data is shared and / or accessed by persons outside of the project team and Charity. For example, a spreadsheet containing names and emails of individuals is accidentally sent to someone outside the organisation who does not have permission to view the file. This section also covers events that may lead to a data breach. In the above example, if the spreadsheet is password protected but still sent to an unauthorised person, this could lead to a breach if not dealt with. Another example of an event that could lead to a potential breach would be if a notebook or memory stick containing personal information is lost or stolen.

23.1. In the event of a data breach or potential breach, this must be communicated to the Chief Executive as soon as possible.

23.2. The Chief Executive will assess the situation and initiate an appropriate plan working with other staff members and external organisations as required.

23.3. 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, etc.

24. Leaving the organisation: should an employee or sub-contractor of the Bridge Group leave the organisation, a plan for secure transfer and / or removal of all files and devices containing sensitive, confidential and / or personal data is to be produced and reviewed by the Chief Executive and quantitative research officer(s).

25. 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.