# Free2B Alliance
# Data protection Policy

Version: 1.2

Date: 27/2/2021

Authorised: Board of Directors

NEXT REVIEW DUE:
Next review period in 5 years – February 2026
Unless an earlier review is triggered by any of the following changes:

- There are changes to operating environment / or strategic direction of the company
- Work behaviour issues that require clarification
- Changes to government policy or legislation

## Contents

## 1 Introduction

This policy clarifies the role of Free2B within the framework of data protection legislation

## 2 Scope of the policy

This policy applies to the processing of all personal data in manual and electronic records kept by Free2B. It also covers Free2B's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of members, supporters, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

The purpose of this Data Protection policy is to enable Free2B to:

- Comply with the law in respect of the data it holds about individuals.
- Follow good practice
- Protect Free2B members, staff, volunteers, supporters and other individuals

Free2B is committed to the lawful and correct treatment of personal, sensitive and commercially sensitive information. This is important to successful working and to maintaining the confidence of those with whom we deal.

## 3 Definitions

*Data Controller:* is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act 1998. This is Free2B.

*Data Protection Officer:* is the person accountable for ensuring that Free2B follows its data protection policy and complies with the Act. Free2B has delegated responsibility to its Principal Lead (Lucie Brooke – lucie@free2b.lgbt). Overall accountability sits with the Board of Directors.

The Data Protection Officer will be responsible for:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Electronic security
- Approving data protection-related statements on publicity materials and letters

*Data Subject:* is the individual whose personal data is being processed. Examples include: employees – current and past; volunteers; job applicants; donors; members; and suppliers.

*Personal Data/Information:* Information that relates to a living person. The Data Protection Act principles do not relate to deceased people, however Free2B would carry out an assessment of any other obligations, legal or otherwise, towards any deceased person before using their information in any way.

The following types of data may be held by Free2B, as appropriate, on relevant individuals:

- client session records
- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

*Sensitive or special Data/Information:* This includes:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Sexual orientation
- genetic and biometric data (where used for ID purposes).

*Processing:* means the use made of personal data including:

- Obtaining and retrieving.
- Holding and storing.
- Making available within or outside the organisation.
- Printing, sorting, matching, comparing, destroying.

Each member of staff and volunteer at Free2B who handles personal data will comply with the organisation's operational procedures for handling personal data to ensure that good Data Protection practice is established and followed. All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Significant breaches of this policy will be handled under Free2B disciplinary procedures.

*Subject access:* Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request, the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more) and certain data may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

4 Key Legislation and Guidance

A number of key pieces of legislation and guidance inform the development of the policies, procedures, guidance and agreements within this document. They include:

- Data Protection Act 1998 (the Act)
- General Data Protection Regulation (effective 25th May 2018)
- Minimum Data Handling Measures (Cabinet Office Standard)
- The Caldicott Report
- Data Sharing Code of Practice (Information Commissioner's Office guidance)
- Common Law Duty of Confidence. This states that data given in confidence should not be disclosed unless:
  - The consent of the individual has been obtained
  - A statute of law dictates that disclosure is made
  - It is in the overriding public interest to do so.

The Eight Principles of Data Protection

The Data Protection Act and Article 5 of the GDPR require that personal data:

P1. Shall be processed fairly, transparently and lawfully. This means Free2B must:

- have legitimate grounds for collecting and using the personal data
- not use the data in ways that have unjustified adverse effects on the Individuals (data subjects) concerned
- be transparent about how Free2B intends to use the data and give Individuals appropriate fair processing notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect
- make sure Free2B does not do anything unlawful with the data.

P2. Shall be obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with those purposes. This means Free2B must:

- be clear from the outset about why Free2B is collecting personal data and what it intends to do with it
- comply with the Act's fair processing requirements – including the duty to give clear fair processing notices to Individuals when collecting their personal data
- comply with what the Act says about notifying the Information Commissioner
- ensure that if Free2B wishes to use or disclose the personal data for any purpose that is additional to, or different from, the originally specified purpose, the new use of disclosure is fair.

P3. Shall be adequate, relevant and not excessive in relation to those purpose(s). This means that:

- Free2B holds personal data about an Individual that is sufficient for the purpose it is holding it for in relation to that Individual
- Free2B does not hold more information than needed for that purpose and has a minimum data set to describe this.

P4. Shall be accurate and, where necessary, kept up to date. This means that Free2B must:

- take reasonable steps to ensure the accuracy of any personal data it obtains
- ensure that the source of any personal data is clear
- carefully consider any challenges to the accuracy of information
- consider whether it is necessary to update the information.

P5. Should not be kept for longer than is necessary. This means that Free2B should:

- review the length of time it keeps personal data
- consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it
- securely delete information that is no longer needed for this purpose or these purposes
- update, archive or securely delete information if it goes out of date.

P6. Shall be processed in accordance with the rights of Individuals under the Act. This means that the Individual has:

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- a right to claim compensation for damages caused by breach of the Act.

P7. Shall be kept secure by the Data Controller and any Data Processor, who take appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information. This means that Free2B and those organisations who process an Individuals data through contracted agreement with Free2B, must:

- design and organise security to fit the nature of the personal data it holds and the harm that may result from an information security breach
- be clear about who in the organisation is responsible for ensuring information security
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff and volunteers
- be ready to respond to any breach of security swiftly and effectively.

P8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals in relation to the processing of personal information.

Processing data with a lawful basis

The GDPR sets out 6 lawful bases for processing personal data. If there is no other lawful purpose identified then consent must be sought. These are:

- Contract: Processing is necessary for the performance of a contract with the Individual, or to take steps to enter a contract. This could be to fulfil an employment contract, or a contract to provide goods or services.
- Legal Obligation: Processing is necessary to comply with a legal obligation
- Vital Interests: Processing is necessary to protect the vital interests of an *Individual* or another person
- Public Task: Processing is necessary to fulfil a task that is in the public interest or in the exercise of official authority vested in the Data Controller
- Legitimate Interests: Processing is necessary for the purposes of legitimate interests of the Association and those legitimate interests are not outweighed by possible harm to the Individuals rights and interests
- Consent: Processing of data has consent from the *Individual.*

What is valid consent?
Consent must be:

- Freely given: the *Individual* has choice and control on how their personal data may be used
- Specific and informed: the *Individual* understands all the purposes for which their data may be used. If there are multiple purposes, consent must be sought for each
- Unambiguous: the *Individual* knows what they have consented to and why, and that they have given their consent

- A deliberate action by the *Individual* e.g. signing / verbal / electronic binary choice options

Procedures

Free2B has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.
- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. Free2B understands that consent must be freely given, specific, informed and unambiguous. Free2B will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

5. Data Collection

Free2B will ensure that data is collected within the boundaries defined within this policy. This applies to data that is collected in person (face to face or over the telephone), electronically

or by completing a form. It applies to any location that is being used by staff, volunteers or contractors to deliver Free2B related business.

When collecting data, Free2B will ensure, wherever possible, that there is a fair processing notice in place and that the *Individual:*

- clearly understands why the information is needed
- understands what it will be used for and what the consequences are should the *Individual* decide not to give consent to processing (more relevant to sensitive information)
- understands who the data may be shared with and why
- has the option to agree to sharing the data
- grants explicit written or verbal consent to collect and share sensitive data wherever possible
- gives explicit consent to contact via email
- is competent enough to give consent and has given so freely without any duress.

The above points indicate that the *Individual* will have enough information for them to give Informed Consent. Any concerns regarding competence should be referred to a health care professional.

There are instances within Free2B where implicit/implied consent is assumed for collecting data, for example information given when responding to an appeal. The Privacy Policy clearly explains this.

6. Data Storage & Security

Information and records relating to *Individuals* will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately in line with the Retention, Archiving and Destruction of Information procedure.

Any recorded information on users/members, volunteers and staff will be:

- Kept in locked cabinets, in locked offices.
- Protected by the use of passwords if kept on computer; with software being kept up to date.
- Appropriate back-up and disaster recovery solutions shall be in place
- Destroyed confidentially if it is no longer needed.
- Archived and stored securely in a locked office, if appropriate.

Access to information on Onedrive or Free2B databases are controlled by a password and only those needing access are given the password. Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Free2B shall promptly assess the risk to the Individual's rights and freedoms and if appropriate report this breach to the Information Commission Office (ICO).

7. Data Access and Accuracy

All *Individuals* have the right to access the information Free2B holds about them and why. Free2B will also take reasonable steps to ensure that this information is kept up to date by asking *Individuals* whether there have been any changes.

If an Individual contacts Free2B requesting information then this is called a 'subject access request'. These will be handled by the Data Protection Officer within the required time limit. Subject access requests must be in writing. Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information. The required information will be provided in 'permanent form' unless the applicant makes a specific request to be given supervised access in person. Free2B may charge a fee of if the subject access request is extensive.

All employees have the responsibility of ensuring information stored about an *Individual* is accurate and relevant to the service provision.

Access to different levels of data is dependent on employee and volunteer role requirements and is detailed in the table below

| Role | Access level |
|---|---|
| Executive Directors | All operational, HR and client data via Free2B database and paper records |
| Non-executive Directors | All operational records<br>Finance records<br>Emergency cover information |
| Payroll administrator | All grant and finance records |
| IT administrator | All database records |
| Youth Service manager | Own HR records, team HR records, client data via Free2B database and paper records |
| Counsellor | Own HR records, client data via Free2B database and paper records and own therapeutic notes kept in line with therapeutic governing body guidance |

| | |
|---|---|
| Community Support workers | Own HR records, client data via Free2B database and paper records |
| Youth worker | Client data via Free2B database and paper records |
| Sessional staff | Paper sessional registers & new members forms |
| Volunteers | Paper sessional registers & new members forms |

In addition, Free2B will ensure that:

- it has a Data Protection Officer with specific responsibility for ensuring compliance with the Act
- everyone processing personal information understands that they are contractually responsible for following good data protection practice
- everyone processing personal information is appropriately trained to do so; is appropriately supervised; will report a suspected or actual breach of data management using the Data Protection Breach Reporting procedure
- anybody wanting to make enquiries about handling personal information knows what to do
- it deals promptly and courteously with any enquiries about handling personal information
- it describes clearly how it handles personal information
- it will regularly review and audit the ways it holds, manages and uses personal information
- it regularly assesses and evaluates its methods and performance in relation to handling personal information
- all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments in the law.

8 Password policy

Every staff member must have a password lock on their screen to protect their data. These should be changed if a security breach has been suspected or occurred. Passwords should be strong and memorable:

- A strong password must be at least 8 characters long
- A strong PIN should contain letters and numbers and be at least 6 characters long
- It should not contain any of your personal information—specifically your real name, user name, or even your company name.
- It must be very unique from your previously used passwords.
- It should contain characters from the four primary categories, including: uppercase letters, lowercase letters, numbers, and characters.

9 Shredding policy

Confidential waste is defined as any personal information that can be used to identify individuals, including their name, address, contact numbers or any financial data. Examples of confidential documentation that you need to dispose of correctly includes: Invoices and quotes.

All confidential waste will be shredded and must not be put into the recycling or main waste collection bins. The pile of confidential waste should be kept securely until it is shredded.

10. Confidentiality

Free2B has a privacy statement for all staff, volunteers and members (clients), setting out how their information will be used. This is shared with everyone on joining and is available on request.

In order to provide some services, Free2B will need to share client's personal data with other agencies (Third Parties). Verbal or written agreement will always be sought from the client before data is shared.

Where an official disclosure request is received, this will only be done after discussions with the Data Protection Officer. All such disclosures will be documented.

11. Transparency

Free2B is committed to ensuring that in principle Data Subjects are aware that their data:

- Is being processed and for what purpose it is being processed.
- What types of disclosure are likely.
- How to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff and sessional workers: via their contact agreement
- Volunteers: via their volunteer agreement
- Members: via their membership form
- Website enquiries: via a website statement (recorded next to each contact form)

Standard statements will be provided to staff for use on forms where data is collected.
We have privacy notices for explaining our use of data for: staff, volunteers, members, members with learning disabilities and website users. The members notice is attached as appendix A and all other notices are available on request.

Data disclosures

Free2B may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties

- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.
- Safeguarding disclosures – where an individual is deemed to be a risk to themselves or others

These kinds of disclosures will only be made when strictly necessary for the purpose.

12. Complaints

If a data subject thinks that their data has been misused or that Free2B has not kept it secure, they should contact Free2B Data Protection Officer (lucie@free2b.lgbt) and tell them (follow Free2B's complaints & compliments policy and procedures).

If the data subject is unhappy with their response or if they need any advice they should contact the Information Commissioner's Office:
https://ico.org.uk/make-a-complaint/

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of Free2B becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, Free2B will do so without undue delay.

13. Staff training and acceptance of responsibilities

All staff who have access to any kind of personal data will be given a copy of the staff handbook and copies of all relevant policies and procedures during their induction process, including the Data Protection policy and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures.

Free2B will provide opportunities for staff to explore Data Protection issues through induction, training, team meetings, and supervisions.
Volunteers will receive information about Data Protection as part of their induction.

Appendix A) Privacy Notice for Free2B members

Personal Data Privacy Notice
Lawful basis for processing data: legitimate interest *

In order to manage and monitor our support services, we keep electronic and paper client files with the above information and we record summary details of all 1:1 and group sessions. This is stored on our database and Onedrive and paper records are stored securely.
Any details which are used for reports (for example, to help us apply for funding) will be made *anonymous* so it does not show who you are.
If you would like to see a copy of your record, please contact Lucie Brooke via email: Lucie@free2b.lgbt

Records will be stored for 7 years after an individual has left our service (or longer where relevant, to ensure an individual is 18 years old before records are deleted) to allow us to meet funder requirements.

Confidentiality Statement
Lawful basis for processing data: Legal Obligation*

Everything we discuss in our 1:1 or group sessions together is confidential except:

1. for the purposes of supervision: Supervision sessions are with Free2B team members and Albany Trust LGBT therapists to allow staff to gain support and guidance in their work and also to check that we are working ethically and competently.

2. where, in our opinion, there may be a danger to yourself or to others. In this situation, we will need to pass information on to ensure we are keeping you and others safe.

* For further information on the lawful basis for processing data please visit the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
If you would like more information, please ask a member of the Free2B Team

Please confirm you have read and understood the above
Additionally, we would like to ask permission to use relevant photographs & / or video images of you on our website and promotional materials.

Aged under 13 parent/guardian consent please check the box to confirm you have read and understood the above

☐ I have read and understood the above information regarding the use and storage of data.

☐ Photography (please leave blank if you DO NOT wish for images to be used).
I agree for Free2B to use photographic/ film images of my child / guardianee in publicity and promotion material including their website. Please note: due to the nature of social media and sharing we cannot confirm exactly when and where photos/film may be used by others.

Parental / Guardian Name Date

Aged 13+ please check the box to confirm you have read and understood the above

☐ I have read and understood the above information regarding the use and storage of data.

☐ Photography consent for individuals aged 16 and above (please leave blank if you DO NOT wish for your images to be used.
I agree for Free 2B to use photographic/ film images of myself in publicity and promotion material including their website. Please note: due to the nature of social media and sharing we cannot confirm exactly when and where photos/film may be used by others.

Date: