DATA PROTECTION AND DATA SECURITY POLICY

1. STATEMENT OF POLICY AND SCOPE OF POLICY

Feed the Homeless Bristol (FTH) is committed to ensuring that all personal information handled by us will be processed according to legally compliant standards of data protection and data security.

The scope is of this policy is to help us achieve our data protection and data security aims by:

1.1 Notifying our volunteers of the types of personal information that we may hold about them and what we do with that information.
1.2 Ensuring volunteers understand our standards for handling personal information relating to volunteers and others: and
1.3 Clarifying the responsibilities of volunteers in respect of data protection and data security.

We withhold the right to amend and update this policy, at our discretion and in line with regulatory change.

Key Term	Definition
Data Protection	the fair and proper use of information about people.
Data Security	the process of protecting data from unauthorised access and only using data for legitimate purposes.
Personal Data	Information about a particular living individual need not be 'private' information, even information which is public knowledge or is about someone's professional life can be personal data.
Data Controller	A controller is the individual or organisation that decides how and why to collect and use the data
Data Subject	The individual whom personal data is about.

2. WHO IS RESPONSIBLE FOR DATA PROTECTION AND DATA SECURITY?

2.2 Maintaining appropriate standards of data protection and data security is collective task shared across the charity. This policy and the rules contained in it apply to all volunteers and trustees alike, irrespective of seniority.

2.3 The board of trustees of FTH has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed Shada Nasrullah as the Data Protection Officer with overall responsibility for data processing and data security.

2.4 All volunteers have personal responsibility to ensure compliance with this policy, to handle all personal information in line with the principles set out here and to ensure that measures are taken to protect the data security.

2.5 Any breach of this policy will be taken seriously and may result in termination of your engagement with FTH.

3. WHAT PERSONAL INFORMATION AND ACTIVITIES ARE COVERED BY THIS POLICY?

This policy covers personal information:

3.1 Which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess.
3.2 Which is stored electronically or on paper.
3.3 Which relates to volunteers (present, past, or future) or to any other individual whose personal information we handle or control – inclusive of our service users.

4. WHAT PERSONAL INFORMATION DO WE PROCESS ABOUT VOLUNTEERS AND WHAT DO WE DO WITH IT?

We collect personal information about you which:

4.1 You provide, or we gather before or during your engagement with us.
4.2 Is provided by third parties, such as references; or
4.3 is in the public domain.
4.4 The types of personal information that we may collect, store, and use about you include records relating to your:
4.5 Contact details as well as contact details for your next of kin, such as telephone, email, internet, fax, or instant messenger use.
4.6 Any matters, grievances, complaints or concerns in which you are involved.
4.7 We confirm that that for the purposes of the General Data Protection Regulation (GDPR) 2016, FTH is a Data Controller, of the personal information in connection with your engagement. This means that we determine the purposes for which, and the way your personal information is processed.
4.8 If you consider that any information held about you is inaccurate then you should tell a Trustee or the Data Protection Officer.
4.9 By providing your personal information to us as part of your engagement with FTH, you **consent** to the use of your personal information in accordance with this policy.

4.10 You hold rights as the data subject to remove this consent at any point or at end of your engagement with FTH.
4.11 Your data will not be sold/shared with third parties for marketing purposes.

5. DATA PROTECTION PRINCIPLES

Volunteers whose role involves processing or accessing personal data relating to other volunteers or service users must comply with this policy and its data protection principles:

5.1 Processed fairly and lawfully. We must always have a lawful basis to process personal information. In most cases, the person to whom the information relates (the data subject) must have given consent. The data subject must be told who controls the information (FTH), the purpose(s) for which we are processing the data and to whom it may be disclosed.

5.2 Processed for limited purposes and in an appropriate way. Personal information must not be collected for one purpose and then used for another. If we want to change the way, we use personal information we must first tell the data subject.

5.3 Adequate, relevant, and not excessive for the purpose.

5.4 Accurate. Checks must be made to update or destroy inaccurate information.

5.5 Not kept for longer than is necessary. Information must be destroyed or deleted when we no longer need it.

5.6 Processed in line with the data subjects' rights. Data subjects have a right to request access to their personal information.

6. DATA SECURITY

We must all protect personal information in our possession from being accessed, lost, deleted, or damaged without proper authorisation, through the use of data security measures.

6.1 Maintaining data security means making sure that:

6.2 Only people who are authorised to use the information can access it.

6.3 Information is accurate and suitable for the purpose for which it is processed.

6.4 Personal informational will disposed of in a confidential and safe manner.

6.5 By law, we must use procedures and technology to secure personal information for the period that we hold or control it.

6.6 Personal data must not be transferred to anyone for processing (e.g., while performing tasks for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

6.7 Security procedures include:

- Physically securing information.

- Any desk or cupboard containing confidential information must be kept locked.
- Computers should be locked with a password or shut down when they are left unattended.

6.8 Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable. Copies held in a cloud storage device will be permanently destroyed upon request.

7. SUBJECT ACCESS REQUESTS

By law, any data subject may make a formal request for information that we hold about them, provided upon receipt of a written request.

Any volunteer who receives a written request should forward it to the Data Protection Officer immediately.