DATA PROTECTION POLICY

Freebridge
COMMUNITY HOUSING

Data Protection Policy			
Last Reviewed	**October 2024**	**Next Review**	**October 2027**
Responsible Officer	**Chief Finance and Technology Officer**		

Policy Statement: Freebridge is committed to complying with all data protection legislation for those individuals that Freebridge collects and processes personal data, so that it may provide its services and support its aims and objectives. Freebridge will comply fully with the UK General Data Protection Regulation and the Data Protection Act 2018.

Freebridge will ensure that the information it holds on its customers, applicants for housing, employees, current and former, are not misused. All personal data held by Freebridge shall be held for a purpose, shall be accurate and, where necessary, kept up to date. All such data shall not be held longer than it is necessary.

Freebridge shall ensure its compliance with the six data protection requirements and be able to demonstrate that all:

1. Processing be lawful, fair and transparent.
2. Purposes of processing be specified, explicit and legitimate.
3. Personal data be adequate, relevant and not excessive.
4. Personal data be accurate and kept up to date.
5. Personal data be kept for no longer than is necessary.
6. Personal data be processed in a secure manner.

Policy Detail:

Background and Scope

This Data Protection Policy sets out how personal data held by Freebridge is accessed, used and maintained. Freebridge Community Housing, as a Data Controller under the law, is registered with the Supervisory Authority, Information Commissioner's Office (ICO), registration Z9425662.

Definitions

There are six main definitions contained in this policy, which are detailed below:

- **Personal data** - means any information that relates to an identified or identifiable living subject i.e. staff member, member of the public, customer, etc. It will generally include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are

members of a trade union, their political beliefs, ethnicity, religion, or sexuality. It can also include an individual's email address or job title if that sufficiently picks them out so that they can be identified (in isolation or with other information that may be held). The above is not exhaustive and any information that relates to an individual can be personal data.

Information about legal entities such as companies is not personal data and falls outside the scope of the legislation. Also anonymised or aggregated data is not personal data (unless you also hold the keys to de-anonymise or de-aggregate it.)

- **Sensitive personal data** – means information about racial or ethnic origin, political opinions, religious beliefs, membership of a trades union, physical or mental health or condition, sexual life, offences or alleged offences or proceedings for any offence committed or alleged to have been committed.
- **Processing** – relates to any activity performed on the personal data. It therefore includes any use, disclosure, storage or collection of personal data, which is held electronically and/or manually.
- **Data Controller** – is the name for an organisation which is ultimately responsible for the processing and the person who controls and benefits from the processing activity.
- **Data Processor** – is any service provider who, in order to deliver services to the Data Controller, processes personal data on behalf of that Controller.
- **Data Subject** – is the individual about whom the personal data relates. Thus individuals who are customers, contacts or clients of a Data Controller are also Data Subjects.

Data Protection Principles

We shall:

Ensure that Freebridge follows the principles for the processing of all personal data and be able to demonstrate its compliance with the following six data protection requirements in order that all:

1. Processing be lawful, fair and transparent.
2. Purposes of processing be specified, explicit and legitimate.
3. Personal data be adequate, relevant and not excessive.
4. Personal data be accurate and kept up to date.
5. Personal data be kept for no longer than is necessary; and
6. Personal data be processed in a secure manner.

We shall also seek appropriate technical and organisation measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

We shall not transfer personal data to any country outside the UK unless that country or territory ensures, in relation to processing of personal data, an adequate level of

protection for rights and freedoms of data subjects acceptable to the UK in relation to the processing of personal data.

Responsibilities:

Freebridge's CFTO shall be the strategic lead for information governance and compliance with data protection legislation and is the primary point of contact for the Data Protection Officer (DPO) for liaison with the Board.

The DPO is a statutory role.

The CFTO is accountable for there being a suitably qualified named DPO at all times; this could be an employee or external service provider, who shall:

- Work closely with the CFTO and his/her team to foster a positive data protection culture within Freebridge;
- Report directly to the Board or a Committee appointed by the Board formally on an annual basis; and
- Lead on all aspects of compliance with data protection legislation within Freebridge.

- Freebridge senior managers responsible for a discrete business area are *Information Asset Owners*. Their role is to understand what personal data (Information Assets) are used in their business area and how it is used, who has access to it and why. They have primary operational responsibility for compliance with data protection legislation and good practice in respect of those assigned information assets.
- Information Asset Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to ensuring that all staff are appropriately trained.
- All employees are responsible for:

  - Checking that any information that they provide to Freebridge in connection with their employment is accurate and up to date.
  - Informing Freebridge of any changes to information, which they have provided, e.g. changes of address, etc.
  - Checking the information that Freebridge will send out from time to time, giving details of information kept and processed about employees.
  - Informing Freebridge of any errors or changes to their personal data.
  - Adhering to data protection guidance set out by the DPO.

Information Asset Register (Data Map)

We shall:

Maintain identified information assets (personal data) in an Information Asset Register (also known as a Data Map). Each processing activity of Freebridge shall be recorded in the Register and detail the lawful basis for that processing.

Privacy Notices and Arrangements:

We shall ensure:

- That no personal data is collected from a data subject without the information required being communicated to the data subject at the time the information is collected; and/or
- That any information required is communicated to them in a timely manner and within one month at the latest.
- Information communicated to data subjects is concise, easily accessible and easy to understand, and that clear and plain language is used.
- Where personal data is collected direct from data subjects, we shall ensure that privacy notices are transparent and clearly detail the purposes the information they provide is to be used.

Data Security

- All employees are responsible for ensuring that:
  - Any personal data which they hold, is kept securely.
  - Personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party; and
  - Any suspected breaches of security are notified to an Information Asset Owner or DPO as appropriate.

  Employees must note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

- Personal information must be:
  - kept in a locked filing cabinet; or
  - in a locked drawer; or
  - if it is computerised, be password protected;
  - kept only on a portable storage device that is itself kept securely;
  - Any data on a portable storage device has to be encrypted in compliance with the Information Communication Technology Policy

Data Subject Requests

- Freebridge recognises the legal rights of the data subjects whose personal data it is processing or intends to process and ensures that appropriate information is provided to them advising them of their rights.
- Freebridge will respond to requests from data subjects in accordance with data protection legislation.

What Happens If a Data Protection Breach Occurs?

Definition:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

General Responsibilities

We shall:

- Take appropriate measures against unauthorised or unlawful processing (including sharing) and against accidental loss, destruction of or damage to personal data.
- Deal with data breaches as required by data protection legislation.
- Maintain a register of all data breaches.

Procedure for Reporting a Data Protection Breach

In the event that someone becomes aware that there has been a potential Data Protection breach, it is essential that they report this on THE SAME DAY. This must be done via email on dataprotectionofficer@freebridge.org.uk.

A brief outline of the breach should be sent in the first instance which should include as a minimum:

When the breach occurred or (the best estimate of when)
The type of information contained in the breach (i.e. home address)
Whether the breach is internal or external
Who the breached data has gone to
Contact details for the next 72 hours for the reportee or a suitably informed delegate

The reason for the urgency is that there is a very short timeframe in which Freebridge is required to inform the ICO.

The DPO will work with the individual to identify:

- The severity of the breach
- The cause of the breach
- The impact of the breach
- The affected subjects of the breach
- How to limit the effects of the breach
- How to prevent a recurrence.

Where a breach is reportable:

It will be the responsibility of the Data Protection Office to ensure the ICO is informed within the required timescales – currently 72 hours for reportable breaches. The Deputy Company Secretary will undertake this in the absence of the DPO.

The circumstances of the reportable breach will be reported as soon as possible to the Chair of the Audit and Risk Committee.

Data Protection and Risk Management by Design

Information Security

Freebridge considers that all data and information is an asset which, like other important business interests, has value to the Association and therefore needs to be suitably protected in respect of its:

- **Confidentiality**: Protecting data and information from unauthorised access and disclosure.
- **Integrity**: Safeguarding the authenticity, accuracy and completeness of information and processing methods; and
- **Availability**: Ensuring that information and associated services are available to authorised users when required.

Data and information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown via pictures, or spoken in conversation.

Freebridge is committed to ensuring that appropriate protection is required for all forms of data and information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations and to meet our duty of care.

We shall:

- Identify potential threats to data, and put in place mitigating practices, weighing up the potential harm and expenditure on controls. .
- Consider the legal, statutory, regulatory and contractual requirements that must be taken into account, including the exchange of data and information from, and to third parties by means of Data Processing and/or Controller-to-Controller agreements and procedures; and
- Identify and assess the principles, objectives and requirements for data processing and use of information that Freebridge has developed to support its operations.

Information Management and Governance: (*Please also refer also to Information Communication Technology Policy*)

We shall:

- Identify systematic, proactive approaches to managing sensitive, confidential information. This approach encompasses people, processes and technology ensuring that information held in manual files and data held on computer records are both secure and available to authorised persons only.
- Ensure that Freebridge's Information Sharing Protocols with key partners, stakeholders and other identified third parties are appropriate and compliant with statutory and regulatory responsibilities.
- Have Internet and Telephony Acceptable Use Rules, and Mobile Device Usage Rules for staff and Board/Committee Members. These will be 'signed up' to as part of the induction information provided to staff and Board/Committee Members on appointment. Staff and Board/Committee Members will be reminded of these policies on a regular basis.
- Ensure, as far as practicable that information held is accurate and up to date, and will check and cleanse data, wherever possible. Where we are requested to erase or port personal data we will do so in a timely manner if appropriate to do so.
- Ensure that data is owned by operational service areas, and relevant managers will take an active role in leading in the use of existing systems, and on projects to implement new systems into their operational area.

Information Security

We shall:

- Monitor our controls in respect of**:**
    - Guidelines on data protection and privacy of personal information.
    - Our use and safeguarding of the Association's records; and
    - Other business and third party responsibilities.

- Identify and utilise those controls that are considered to be common best practice for information security including:
    - Use of data and information security guidance.
    - Allocation of data and information security responsibilities.
    - Data and information security education and training.
    - A procedure for reporting data breaches, security incidents and near misses*;* and
    - Business continuity management.

Tracking of records and security

We shall ensure:

- The tracking of appropriate records usage within records and documentation systems.

- Only those users with appropriate permissions are performing records tasks for which they have been authorised.
- All data and personal records ranging from a handwritten note to an automated transaction in an electronic document management system are appropriately controlled and are traceable.

Electronic records and authenticity

We shall ensure:

- That security measures include:

  - Digital signatures to protect the authenticity and integrity of electronic documents; and
  - Scanning and storing of electronic data, records and digitised documents in such a way as to ensure their authenticity in the event of a legal challenge.

Classification of data and information for business purposes
Classification of data, records and information shall determine how this information is to be handled and protected from unauthorised access, loss or damage.

Security of Highly Sensitive/Confidential Personal Information

Security requirements are the same for all such records, irrespective of format. If a record contains confidential material, then it must be maintained and disposed of securely i.e. only authorised persons should be allowed access to it.

We shall: Ensure the security of confidential records as follows:

<u>Paper records</u>

- Confidential records should carry an appropriate classification label.
- File titles should be worded so that confidential information (e.g. someone's address, phrases such as "vexatious tenant") is not included in the title.
- Clear desk arrangements should be promoted by Information Asset Owners as standard practice i.e. when the member of staff is out of the office, any confidential data should be removed from the desk top and locked away.
- Filing cabinets containing confidential material should be locked at all times when not in use.
- A list of persons authorised to access and/or maintain confidential records should be kept and reviewed regularly.
- Faxes may not be secure, so faxes should not be used to transmit confidential information.
- Non-current records which need to be kept for a specified period should be transferred to a secure storage facility. Security of records in transit should be ensured.

Electronic records

- Access to confidential records should be restricted i.e. access to drives/files and/or password protected; as well as access and authorisation levels being clearly documented so that when people may leave that information does not become in accessible.
- Workstations should be locked when not in use.
- When using mobile computing facilities such as laptops, special care should be taken to ensure that confidentiality is not compromised (e.g. through overlooking by members of the public), and that back-ups and virus protection are regularly undertaken via ICT.
- All employees should view the use of standard Email as an unsafe method of transmitting personal data i.e. because of the risk of sending it to the wrong recipient (or multiple recipients) or from hacking/theft of information via the system/web usage. Staff should be aware of this when using email to transmit confidential information. Arrangements should be made for relevant emails to utilise either Secure File Transfer Protocols (SFTP) or the Ministry of Justice's Criminal Justice Secure Email (CJSM) systems or via Mimecast Secure Email arrangements
- All removable media such as USB Data sticks etc should be stored in a safe, secure environment.

Destruction of confidential data

- All employees have a responsibility to consider security when disposing of information in the course of their work.
- For destruction of material in paper format all *confidential paper records* shall be disposed of in the confidential waste bins provided for shredding.
- Care must be taken with destruction of electronic records, which can be reconstructed from deleted information. Erasing or reformatting computer disks or personal computers with hard drives that contained personal information shall be carried out in collaboration with the ICT Support team.

  (Refer also to *Information Communication Technology Policy*: *Business and personal mobile devices with company data on them/access to corporate systems will be passcode protected as a minimum.*
  All data and access will be 'wiped' remotely if a device is lost or stolen. With personal devices some asset management responsibility passes to the individual. However, we will insist on up to date security standards and updates being applied to devices).
- All destruction, of information in any medium, should be carried out in accordance with the provisions of our current records retention schedule for those records, so that a proper audit trail can be kept.

Retention of Data

We shall ensure:

- Freebridge's retention arrangements do not retain personal data for any longer than is necessary for legal or regulatory reasons or for its legitimate organisational and business purposes.
- Freebridge shall comply with the National Housing Federation data retention schedule.
- Timely and appropriate disposal at the end data's useful life through risk assessed measures, such as erasure or anonymisation.
- Where personal data is to be transferred for long-term preservation (for example where it is of value for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) Freebridge ensures that appropriate technical and organisational measures safeguard the rights and freedoms of living individuals.

Contractual Arrangements with Contractors and Other Organisations (Processors)

Freebridge ensures through its procurement and data protection contract arrangements that we shall only engage with those contractors and other organisations (who may process personal data on our behalf) that provide a sufficient guarantee of technical, physical and organisation security and be subject to a written contract.

Freebridge shall also undertake an assessment of appropriate security arrangements as part of due diligence before any data processor is engaged and that where appropriate seek business assurance of those security arrangements is conducted before entering into the contract.

Data Protection Impact Assessment (DPIA)

Freebridge shall ensure that risk-based Data Protection Impact Assessments (DPIA) are undertaken that ensure that issues of data quality and accuracy are taken into account, when appropriate, for new contracts or projects.

Data Quality

Freebridge shall ensure that personal data is accurate and where necessary kept up-to-date and that where personal data is found to be inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Closed-circuit Television (CCTV)

A protocol will be developed to direct the Association's use of CCTV cameras.

Training and Awareness

We shall ensure:

That employees and other workers receive appropriate training, are competent in and understand the data protection responsibilities assigned to them**.**

The DPO shall ensure that the elements of data protection training programme are kept up to date.

Conclusion

Compliance with the Data Protection Act 2018 (DPA18) and the UK GDPR is the responsibility of all employees and non-executive directors of Freebridge. Any deliberate breach of the data protection policy and procedures may lead to disciplinary action being taken, or access to Freebridge facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy and procedures should be taken up with the DPO and/or Chief Executive.