Dunbritton Housing Association Limited

Name of Policy	**Privacy Policy**
Responsible Officer	**Corporate Services Manager**
Date approved by Board	**November 2023**
Date of next Review	**November 2026**
Section	**Corporate Services**
Reference	**C17**

We can produce information, on request, in large print, Braille, tape and on disc. It is also available in other languages. If you need information in any of these formats, please contact us on 01389 761486

Contents.

1. Introduction

Dunbritton Housing Association (DHA) is committed to ensuring the secure and safe management of data held in relation to customers, staff, and other individuals. All staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with our procedures. This Policy sets out our duties in processing this data.

DHA gathers and uses information about individuals. This can include customers (tenants, factored owners etc.), employees and other individuals that DHA has a relationship with. The data we collect and manage contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

2. Legislation

We are required in accordance with the relevant legislation to process data safely and correctly. The relevant legislation includes:

- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
- The Freedom of Information (Scotland) Act 2002

3. Data

3.1 DHA holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held, and processed by the Association, for customers, is detailed within our 'Fair Processing Notice'; and employees will also be issued with a FPN and an addendum to their contract of employment 'Personal Data' – a person can be identified by that data alone, or in conjunction with other data held by the Association. This data may also include information that is sensitive in nature. (i.e., relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

4.1 DHA is permitted to process Personal Data on behalf of data on the following grounds:

- With the consent of the data subject.
- Entering into or the performance of a contract
- Compliance with a legal obligation.
- To protect the data subject or another person.
- A task carried out in the public interest or in the exercise of the Association's official authority, or Legitimate interests.

4.2 Fair Processing Notice (FPN**)**

- The FPN will be provided to the customer from the outset of processing their Personal Data.

4.3 Employees

- Details of data held, and processing of that data, is contained within the Employee FPN.
- A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Corporate Services Manager.

4.4 Consent

- Any consent obtained by the Association must be freely given and for a specific and defined purpose. All consent will be acquired in an 'opt-in' format and the data subject will be advised as to how they can withdraw this consent.

4.5 Processing of Special Category Personal Data or Sensitive Personal Data In these circumstances DHA must process data when necessary:

- For carrying out obligations or exercising rights related to employment or social security.
- To protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person.
- For the establishment, exercise, or defence of legal claims, or whenever court are acting in their judicial capacity; and
- For reasons of substantial public interest.

5. Data Sharing

5.1 DHA shares its data with various third parties for numerous reasons in accordance with our relevant policies and procedures. To ensure compliance with GDPR by third parties we will enter into Agreements which govern the processing of data, security measures to be implemented and responsibility for breaches.

6. Data Processors

6.1 A data processor is a third party that processes personal data on behalf of the Association. They must comply with GDPR and ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.

6.2 If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors. Where DHA contracts with a third party to process personal data held by us, we shall require the third party to enter into a Data Protection Addendum with the Association.

7. Data Storage and Security

7.1 All Personal Data held by the Association will be stored securely, whether electronically or in paper format and safely disposed in line with the Association's storage and disposal procedures.

8. Breaches

8.1 A data breach can occur at any point when handling Personal Data and the Association will implement its Data Breach Procedures as and when required.

9. Data Protection Officer (DPO)

9.1. DHA will appoint a Data Protection Officer who will have responsibility to ensure that we are compliant with the GDPR. This role will include compliance and liaison with the Information Commissioner's Office (ICO).

10. Data Subject Rights

10.1 DHA will ensure in its procedural guidelines that it fully complies with all rights and responsibilities that are provided to individuals under the GDPR. These will include:

- Subject Access Requests
- The Right to be Forgotten.
- The Right to Restrict or Object to Processing

11. Privacy Impact Assessments (PIAs)

11.1 DHA will implement PIAs to mitigate against potential 'high risks' that our operations may have on personal privacy. When required we will consult with the ICO where a 'high risk' cannot be reduced. The DPO will have responsibility for the reporting of these matters within the required timescales.

12. Archiving, Retention and Destruction of Data

12.1 DHA will ensure that all Personal data is archived and destroyed in accordance with the relevant departmental and legal procedures.

13. Use of Dunbritton Electronic Devices

13.1 As part of our day to day work, staff will have access to electronic devices which can store data, notably tablets, mobile phones and desktop PCs.

13.2 These devices remain the property of Dunbritton.

13.3 All staff note that it is a requirement of using these devices that they accept that all data stored within these devices is deemed to be owned by Dunbritton.

13.4 No staff member should save images or data of any sort on these devices which are not for work purposes.

13.5 Any data stored within these devices could be accessed by any member of staff, for the purposes of day-to-day work, monitoring of performance, monitoring of quality of work, and for disciplinary purposes.

13.6 Staff wishing to store private personal information should do so using the secure H drive but must be aware that this data may still be accessible.

13.7 Any requests to access secure areas, such as individuals H drive, must be authorised by the DPO and Chief Executive Officer and must first follow a data impact assessment.

14. Use of Dunbritton E-mail accounts

14.1 All Dunbritton staff will have access to a Dunbritton e-mail account. These are for the purpose of carrying out their day-to-day tasks.

14.2 All staff members must ensure that these accounts have the appropriate disclaimers attached when corresponding with parties out with the Association.

14.3 Through using these accounts, staff members may give the impression that they are acting on the association's behalf. Where there is a possibility of confusion over the capacity or nature of the correspondence, staff must ensure it is clear when they are not acting in an official capacity. Anyone found to be acting in this manner may be subject to the code of conduct.

14.4 Whilst it is accepted there may occur reasonable fair use of these accounts for personal contact, this is only allowed on the understanding that this information may be subject to any subject access request, freedom of information request, or required to be accessed or monitored as part of the Association's business.,

14.5 For these reasons, all staff members are asked not to use the Dunbritton e-mail account for any correspondence that is personal, private or sensitive in nature.

14.6 We expect all staff representing Dunbritton to act in a courteous and professional manner when communicating with our customers and contractors and this includes any written correspondence, including e-mails.

14.7 When a staff member is off sick with no clear return date, and there is a risk that e-mail contacts may be missed, the manager will seek permission from the CEO to access the staff members e-mail account. This will be for the purposes of ensure no new contacts are missed and that any contacts have been followed up on. Through this policy, all staff will be deemed to be aware of this process.

14.8 Where a manager has a concern over inappropriate use of an e-mail account, they this includes checking of performance, ensuring contacts are maintained, ensuring works are completed, disciplinary matters, and any other fair reasons they may request access to the account through seeking the agreement of the DPO and Chief Executive Officer. In such circumstances a data risk assessment shall be carried out which looks to balance the urgency of the concern with the staff members rights to privacy. Any access will be required to be balanced by these needs and limited accordingly.

14.9 Any e-mail monitoring will be proportionate and for a clear purpose. It will only look at relevant and recent communications. It will only be authorised where there is no other reasonable and less intrusive means to achieve the stated aims and it shall be only for the minimum amount of time required to achieve these aims.

14.10 Special care will be taken when monitoring e-mail data not to access any information that is clearly personal and private, especially information labelled private or confidential or any correspondence between staff and trade union representatives, legal representatives, or between colleagues over matters regarding representation in the workplace.

14.11 No automated monitoring will be used without the agreement of the DPO and a reflective update of this Policy.

14.12 Any internal e-mail correspondence between colleagues, shall be treated as private and confidential unless one of the parties raises a concern with regard to its content or its title or any apparent attachment cause the DPO to believe there may have occurred significant malpractice.

14.13 Any external e-mails which are clearly from a medical professional, financial institution, or through their title or correspondence address, are evidently not sent or received with regards to DHA business shall be treated as private and confidential unless one of the parties raises a concern to DHA over its content, or its title or any apparent attachment cause a manager to believe there may have occurred malpractice.

14.14 Whilst it is strongly recommended that all correspondence between staff and their trade union representative or between staff seeking to organise for trade union purposes are not sent via work e-mails, all such correspondence shall be treated as private and confidential.

15. Equality and Diversity

13.1 As a service provider and employer we recognise the requirements of the Equality Act 2010, oppose any form of discrimination, and will treat all customers, internal and external, with dignity and respect. We recognise diversity and will ensure that all of our actions ensure accessibility and reduce barriers to employment and the services we provide.