



Dunbritton Housing Association Limited

Name of Policy	Usage of Electronic Devices and Email Policy
Responsible Officer	Finance & Corporate Services Manager
Date approved by Board	June 2024
Date of next Review	June 2027
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.

Section		Page
1.	Introduction	3
2.	Legislation	3
3.	Use of Dunbritton Electronic Devices	
4.	Use of Dunbritton Email Accounts	
12.	Equality & Diversity	

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 processes 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 category personal data under the UK GDPR).

2. Legislation

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

- The UK General Data Protection Regulation (UK GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
- The Data Protection Act 2018The Freedom of Information (Scotland) Act 2002
- The Environmental Information (Scotland) Regulations 2004
-

3. Use of Dunbritton Electronic Devices

3.1 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.

3.2 These devices remain the property of Dunbritton.

3.3 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.

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

3.5 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.

3.6 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.

3.7 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.

4. Use of Dunbritton E-mail accounts

4.1 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.

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

4.3 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.

4.4 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, environmental information request or similar and / or be required to be accessed or monitored as part of the Association's business.

4.5 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

4.10 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.

4.11 No routine monitoring will be used without the approval of the DPO.

4.12 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.

4.13 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 insofar as it relates to individuals rather than DHA.

5. Equality and Diversity

5.1 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.

