Dunbritton Housing Association Limited

Name of Policy	Data Management Policy
Responsible Officer	Corporate Services Manager & Data Protection Officer
Date approved by Board	August 2021
Date of next Review	August 2024
Section	Corporate Services
Reference	DM1

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

1.1 This policy sets out our approach to the provision, management and security of Dunbritton Housing Association's (DHA) data. DHA recognises it has obligations and legal responsibilities to protect the rights of individuals who have given information to the Association. This includes Board Members, employees, shareholding members, tenants, housing applicants and factoring customers. DHA will make all reasonable efforts to comply with requests covered by the legislation within the agreed time frames; and act in a manner that is open and honest, and where practical, proactive. Further we will ensure that all requests for information are handled in line with current best practice and that they are processed effectively and efficiently in complete confidentiality.

1.2 This document has been created under the following legislation:

- The General Data Protection Regulation (GDPR)
- Data Protection Act 1998.
- Freedom of Information (Scotland) Act 2002 (FOI).
- Environmental Information (Scotland) Regulations 2004.

1.3 This policy will be reviewed every 3 years by the Corporate Services Manager & the Data Protection Officer and any significant changes will be reported to the Board.

2. Data Management

2.1 As a holder of customers' data, DHA will be classed as a Data Controller. GDPR requires Data Controllers to meet certain obligations when processing personal information to prevent that information being improperly used or distributed. The individual whose personal details are being held also has a right to know exactly what information is being held about themand why it is held.

3. Responsibilities

3.1 Ultimate responsibility for implementing the law lies with DHA's Board. The Chief Executive Officer (CEO) has been delegated by the Board to oversee the data practices within the office. Line managers are responsible for ensuring that this policy is adhered to and for building up good practice as required. Staff are ultimately responsible for ensuring that they are acting in line with this Policy and within the law.

4. Information Commissioners Office (ICO) Registration

4.1 DHA must notify the Information Commissioner of their holding of personal data (also called registration). Registration must be updated annually at the beginning of October.

5. Data Principles

5.1 GDPR provides principles that organisations must adhere to when using and processing individual's data. The Principles state that personal data must be:

- Processed fairly and lawfully and in a transparent manner.
- Processed for the purpose for which it was obtained.
- Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Accurate and where necessary kept up to date.
- Not be kept for longer than is necessary for that purpose or those purposes.
- Processed in accordance with the right of data subjects under law.
- Protected by appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and prevent accidental loss or destruction of, or damage to, personal data.
- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects.

6. Processing Data

6.1 Processing of data is the obtaining, recording, holding, organising, adapting, consulting, retrieving, disclosing or destroying of personal information. In practice when processing data an organisation 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 concerned.
- Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data.
- Handle personal data only in ways they would reasonably expect; and not do anything unlawful with the data.

When considering the processing of personal data a distinction must be made between ordinary data and sensitive data as each type may only processed under specific conditions.

6.2 Consent for the processing of data must be explicitly given, specific, and informed. The individual must be made aware of precisely what information is being

processed, why and what specific use will be made of that information by any third party to whom it is to be disclosed. The terms for which we hold information are provided for in our Fair Processing Notice (FPN). We shall ensure that all data subjects receive a copy of this FPN prior to our holding their data.

6.3 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.4 The measures must ensure a level of security appropriate to the harm that might result from breach of security and the nature of the data to be protected. The state of technology and the costs of implementing any measures should be taken into account. DHA must also take reasonable steps to ensure reliability of staff having access to data and ensure that they are trained appropriately.

7. Disclosure of Data

7.1 The Association must ensure that personal data is not disclosed to any unauthorised third party, which includes family members, friends, and government bodies. All staff and Board members should exercise caution when asked to disclose personal data held to a third party, and where possible, such requests should be submitted via the Data Protection Officer.

7.2 DHA will hold Data Sharing Agreements with third parties that we are required to share data with, , data may be shared with these parties in line with the FPN. Care should still be exercised with regards to sensitive data such as information on disability or sexuality.

7.3 When members of staff receive enquiries about a named customer (shareholder, tenant, waiting list applicant, sharing owner or factoring customer), the enquirer should be asked why the information is required. If the enquirer is not a 3rd party with a Data Sharing Agreement, care shall be taken to ensure that the party has clear consent. Where this is not the case the enquiry should in the first instance be passed to the Data Protection Officer.

7.4 The Data Protection Officer will ensure that any information sharing is carried out in accordance with the principles of GDPR.

8. Mandates

8.1 Occasionally a Data Subject may instruct a party to act on their behalf. If the party is available, such as during a phone call, then an oral mandate may be taken to speak with regards the case on the Subject's behalf. Care should still be taken with regards to sensitive data. If the mandate is provided in writing, this mandate must clearly show that the subject is happy for the party to act on their behalf with DHA and that the subject is aware that their data will be shared. If the mandate does not clearly set this out, the party may be asked to seek a new mandate.

9. Subject Access Request (SAR) - Requests from an individual to view Personal Data

9.1 Any request for personal information held by DHA must be passed to the Data Protection Officer. When receiving a request for personal data staff shall establish:

- What information is sought (It is important to be concise with regards this to reduce providing unnecessary data)
- If there is a specific time period for the information sought (e.g. correspondence in the last three weeks)
- How the party wishes to receive the data (e.g. e-mail)

9.2 Identification should be sought to confirm that the party seeking the data is the individual on which the data is held. This may be done through checking ID or asking security questions.

9.3 Information disclosed will:

- Be specific to the individual.
- May include both computer and highly structured manual records.
- Not disclose the identity or personal data of any other individual e.g. in the case of anti-social behaviour complaints this should be redacted prior to disclosure.
- Have all jargon and codes clearly explained.

9.4 All SAR's will be responded to within 40 calendar days from the date it was received in the format requested by the Data Subject.

10. Requests from third parties - For information received from MPs, MSPs and local councillors on behalf of constituents

10.1 Elected Members had privileges granted upon them by the Data Protection (processing of sensitive personal data) (Elected Representative) Order 2002.

10.2 DHA recognises the important role Elected Members provide in assisting our customers and efforts shall be taken to assist such enquiries.

10.3 Where an elected official requests access to sensitive data, or if there are any concerns with regards to providing access to data under the 2002 Order, the matter shall be considered by the Data Protection Officer.

11. Retention of Data

11.1 DHA will identify the minimum amount of information that is required in order to fulfil its purpose and statutory duties. If the information is kept longer than necessary then it may become irrelevant and excessive. For this reason audits will be carried out of the information that we hold not only to ensure that it is up to date but also to enable it to identify information that is no longer relevant.

11.2. Data Subjects have the right to have their data amended to address any error. Where a data subject contacts the Association to amend an error they should be put in contact with the Data Protection Officer. When the data requires to be amended urgently, this shall be done, but a note of the new and previous data shall be supplied to the Data Protection Officer.

11.3. We shall ensure that data is only held for the purpose for which it was collected. Once this purpose has been completed, notably through completion of contract, we shall only retain this information for a period to ensure we meet legal requirements or where there is a financial or legal risk. We recognise that the Data Subject may in some circumstances have a right to be forgotten. Where a Data Subject contacts DHA to exercise this right, their details shall be taken and provided to the Data Protection Officer who shall check and carry this out.

11.4 We will take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. We will ensure that all staff are trained appropriately.

12. Breaches of Confidentiality

12.1 An individual can apply to the Information Commissioner Office (ICO) for an assessment as to whether it is likely or unlikely that the processing of personal data by DHA breaches confidentiality.

12.2 The ICO can place an enforcement notice upon the Association and require DHA to take or refrain from taking specified steps when processing data. Failure to comply with an enforcement notice is a criminal offence. If a staff or Board member has been found to breach confidentially whether deliberate or inadvertent it will be treated seriously and acted upon rigorously. An alleged breach of confidentiality by either a staff or Board member will initiate a thorough investigation with appropriate action to follow.

13. Equality & 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.

Data Management Staff Agreement Proforma

I have read and understood Dunbritton Housing Association's Data Management Policy and agree to abide by the procedures stated therein, particularly in relation to:

- Communications including E-Mail, Internet & Social Media Usage
- GDPR
- Data Protection
- Access to Information
- Maintaining data audits
- I.T. Security

Name: _____

Job Title: _____

Date: _____

Signature: _____