Bridgewater Housing Association Policy

Policy name	ICT Document Management Policy
Policy category	Finance and ICT
Policy number	FS14
Date adopted	
Last review	-
This review	19th February 2025
Next review	September 2027
Equalities impact assessment required	No
Links to other documents	• Electronic Communications Policy • Data Retention Procedure
Consultation	Internal - This policy was issued to the leadership team for comment.
Need for Procedure	Within this document
Policy Owner	Head of Finance and IT

This policy can also be provided in large print, braille, audio, or other non-written format and in a variety of languages on request. Please contact the Association by emailing admin@bridgewaterha.org.uk or call 0141 812 2237 to request this.

1. Introduction

This policy is to ensure that documents held by Bridgewater are held in a consistent and secure way that is easily retrievable by the relevant people, and which allow easy access to information. Documents will be stored in a way that will ensure they are easily shared with staff and the Board and compliant with general data protection regulations (UK GDPR) and Freedom of Information access (FOI).

The Policy will:

1. Provide a cohesive guide to how to store documents.
2. Co-ordinate all the different types of storage, that is, make sure all staff know
3. Outline the different storage needs for each Department.
4. Ensure all staff are fully trained and aware of the Document Management Strategy.
5. Outline review and monitoring processes.
6. State who is responsible for updating the Strategy.

2. Aim and Objectives

This policy aims to establish an online first basis for the storage of documents, in particular making use of SharePoint and Teams, whilst recognising the requirement of local storage as made necessary by some applications. The Association will aim to be majority online cloud storage oriented for files by the financial year 2026.

3. Overview

The Association has several robust and reliable data storage systems in place, including local systems as well as cloud storage. To enable maximum efficiency and to continue to move away from paper-based storage towards digital storage of files and data, the Association will continue to invest in and provide training on the various document management abilities it has in place.

4. Current Storage Methods

4.1 Windows Explorer (File Server)

The Association uses various departmental shared “drives” to store many of its working documents. Each directory has been set up to ensure that the files are stored in an easy to understand, easily accessed format. Where necessary, folders may be accessed by multiple departments depending on access privileges assigned.

Our Data Retention Procedure will tell staff when they can delete documents.

4.2 SDM

SDM is the main housing management database for Bridgewater's tenants and owners. SDM generates most of the letters, statements and invoices sent to owners and tenants. These are stored by attaching them to a diary entry in the tenant or owner file. Letters that are not generated in SDM but relate to tenants or owners will be stored in the SDM storage system and attached to a diary entry.

The SDM Document Management System is a filing system for each tenant/owner. All letters, documents and invoices including scanned forms and correspondence are held in SDM. Also, any documents that can be attached to a property file are held in SDM.

4.3 My Home (My BHA)

Tenants and Owners can view documents that are stored in the SDM Document Management System, if they register and log in to My BHA. They will not see sensitive documents but will see all other letters and scanned documents. For the avoidance of doubt, documents have a default status of sensitive and will only be marked non-sensitive (i.e. viewable by the customer) if the staff member processing the document is 100% sure it should be shared with the customer.

4.4 SharePoint/Teams

Board members and staff can access documents on Microsoft SharePoint, which also incorporates Microsoft Teams. This includes Board Papers, their library of documents and the Association's Policies and Procedures. Board members may access documents through their tablets or personal device, if granted, and therefore all documents stored here should be converted to PDF or Word wherever possible to allow them to use Adobe Acrobat or Office tools to access the documents. Private board member workspaces and multi factor authentication for staff are the methods used to protect the data stored. SharePoint document storage also extends to the use of Microsoft OneDrive and Microsoft Teams, both of which are built upon the SharePoint platform. Staff members may use these platforms to store information that is specific to them or their role for the sole purpose of being able to see and work upon these documents from multiple locations.

To enable superior collaboration and for ease of access, the Association is migrating the majority of its working documents to SharePoint/Teams, whilst critical access documents which are required to be accessible by software such as SDM, Sage Accounts, Sage Payroll, will continue to be stored on locally shared server folders/drives.

2.5 E-mail

Staff and Board members store information in their e-mail folders. Folders are the responsibility of the individual and are required to be held in such a way that they can be retrieved easily if there is a data subject access request. E-mails should not be held beyond their usefulness or beyond the timescale set out in the Data Retention Procedure and therefore staff should delete unnecessary files at least annually, although quarterly is recommended. Security on phones, home laptops and other remote devices is essential, and all Board and staff must abide by the mobile device procedures and the Data Protection Policy and procedures. All access to the Association email systems by staff is controlled by multifactor authentication. When sharing files via email, staff are encouraged to instead provide a link to the network or cloud location of the document rather than simply attach the document to reduce further duplication of data.

2.7. Website

The website has become a vital storage area for Tenants and other stakeholders principally due to the introduction of Freedom of Information. There are strict protocols in place to ensure that the information held on the website is recorded on the Guide to Information and is up to date. It should be held on the site in accordance with the data retention procedure.

2.8 External Storage (Memory sticks, external hard drives etc.)

The use of external storage is discouraged upon the Association's devices and networks and, as such, digital policies are in place to require these types of storage location to be encrypted, otherwise their functionality will be prohibited. Where these devices are in use, the quality and accuracy of data must comply fully with the Association's data retention schedule, and disposal of these devices must be subject to certification from a recognised party.

5. Protocol

5.1 Dating Folders

Digital folders which have a date of relevance must be dated in line with the current financial year and not that of the calendar year.

5.2 Avoidance of Duplication

Data on any system should not be stored twice. If a document is to be shared by several people or departments, everyone involved will know where it is held and work on the same document, not save a copy elsewhere to work on. For example, policies should be worked on in the policy folder. Draft Policies should be named with the letter "b" after the reference number.

5.3 Personal drives ('H' Drive)

Staff can store documents in their H drive such as personal information. If they are working on a document and do not want anyone else to access the document, it can be saved in the H drive. Once it is ready to share, it should be moved to the appropriate departmental drive. Local drives will be moved to OneDrive.

5.4 Sub-folders

Sub-folder structures should be easy to access, so that retrieving documents involves as few clicks as possible to find a document. It is the responsibility of the senior manager of the section to review the number of sub-folders to ensure easy access.

6. Permission

Each storage system has controls to ensure that the folder structures, permissions and indexing are maintained correctly. Permissions are administered by the IT Manager, IT Assistant or external support provider.

6.1 Windows Explorer

The top-level folder structure is set up by the IT Manager under the guidance of the Leadership Team and cannot be changed by anyone else.

6.2 SDM

The SDM folder structure is set up by the Leadership Team (tenants and property file) and the Property Management Officer (owners). This will not be amended without permission from the appropriate person.

7. Monitoring and Review

This Document Management Strategy Policy will be reviewed every three years, or when there are substantial changes to legislation such as UK GDPR or FOI, whichever comes first.

8. General Folder Structure – Local and Microsoft Teams

The below folder list outlines the primary groups who have access to networked and cloud-based (online) folders. It does not include sub-folders, or specific working groups which are subject to change regularly. Where the term Local Share is used, this refers to the presence of a shared departmental folder within the Association’s local servers. Teams refers to a cloud based “Team” workspace which includes the availability of shared files.

Folder	Location(s)	Permissions
All Staff	**Teams**	**CEO, Leadership Team, Corporate Services, Finance, Customer Services, Property Services, Care and Repair**
Board Portal	**Teams**	**CEO, Board, Leadership Team, Corporate Services**
Leadership Team	**Teams**	**CEO, Leadership Team**
Corporate Services	**Teams and Local Share**	**CEO, Corporate**

		Services
Finance	**Teams and Local Share**	**Finance**
ICT	**Teams**	**Finance, ICT Team, External Support Provider**
Housing	**Teams and Local Share**	**Housing Services, Customer Services**
Customer Services	**Teams**	**Housing Services, Customer Services**
Property Services	**Teams and Local Share**	**Property Services**
Factoring	**Teams and Local Share**	**Property Services**
Care and Repair	**Teams and Local Share**	**Care and Repair**