Belmont House, 57 Belmont Road, Cambuslang, G72 8PG
www.wwhc.org.uk E: enquiries@wwhc.org.uk T: 0141 641 8628

Policy Name	**Information Security Policy**
Policy Author	**DPO / Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**March 2026**
Latest date of Next Review	**March 2029**

West Whitlawburn Housing Co-operative will provide this policy on request at no cost, in larger print, in Braille, in audio or other non-written format, and in a variety of languages. Please contact the office.

HAPPY TO TRANSLATE

Registered with the Scottish Housing Regulator No. 203
Registered Charity No. SCO38737, VAT Registration No. 180223636
Registered society under the Co-operative and Community Benefit Societies Act 2014

1 Introduction

1.1 West Whitlawburn Housing Co-operative (WWHC) are committed to the highest standards of information security.

1.2 Data protection legislation requires us to:

1.2.1 use technical and organisational measures to ensure personal data is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

1.2.2 implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data protection compliance measures into our personal data processing activities; and

1.2.3 demonstrate that we have used or implemented such measures.

1.3 The purpose of this Policy is to:

1.3.1 protect against potential breaches of confidentiality.

1.3.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse.

1.3.3 supplement our Data Protection Policy to ensure that all staff are aware of and comply with data protection legislation as part of their roles at our organisation; and

1.3.4 increase awareness and understanding within the organisation of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the personal data that they handle and use as part of their roles.

1.4 This Policy supplements our Data Protection Policy and other relevant procedures (including the Data Breach Management Procedure) and transparency statements, and the contents of those policies and statements must be considered, as well as this Policy.

1.5 WWHC's information assets are recorded at Appendix 1 of this Policy.

2 Definitions

For the purposes of this Policy:

business information	means business-related information, other than personal data relating to housing applicants, our tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members;
confidential information	means trade secrets or other confidential information (either belonging to us or to third parties); and
personal data	means information relating to an individual who can be identified (directly or indirectly) from that information.

3 Roles and responsibilities

3.1 Information security is the responsibility of all our staff. Our Data Protection Officer (DPO) is responsible for:

3.1.1 monitoring and implementing this Policy.

3.1.2 monitoring potential and actual security breaches.

3.1.3 ensuring that staff are aware of their responsibilities through training and issuing guidance and communications to them; and

3.1.4 ensuring compliance with data protection legislation and guidance issued by the Information Commissioner's Office.

4 Scope

4.1 The information covered by this Policy includes all written, spoken and electronic information held, used or transmitted by or on our behalf, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2 This Policy applies to all staff.

4.3 All staff must be familiar with this Policy and comply with its terms when undertaking their roles with the organisation.

4.4 Information covered by this Policy may include:

4.4.1 personal data relating to housing applicants, our tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members.

4.4.2 other business information; and

4.4.3 confidential information.

5 General principles

5.1 All WWHC information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2 Personal data must be protected against unauthorised and / or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5.3 Staff should discuss with the DPO the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information that they access as part of their roles at the organisation.

5.4 WWHC's information is owned by the organisation and not by any individual or department within the organisation. Our information must be used only in connection with work being carried out for the organisation and not for other commercial or personal purpose.

5.5 Personal data must be used only for the specified, explicit and legitimate purposes for which it was collected in accordance with data protection legislation.

6 Information management

6.1 Personal data must be processed in accordance with:

6.1.1 the data protection principles, set out in our Data Protection Policy; and

6.1.2 all other relevant policies.

6.2 We will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

6.3 Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with our Data Retention Policy.

7 Human Resources information

7.1 Given the internal confidentiality of personnel files, access to such information is limited to line managers and the Director. Other staff are not authorised to access this information.

7.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information to which they have access strictly confidential during the recruitment process and must pass this to the Director once the recruitment process is complete.

7.3 Staff may ask to see their personnel files and any other personal data in accordance with their rights under data protection legislation. Further information is contained in our Response Procedures for Data Subject Requests and from our DPO.

8 Access to offices and information

8.1 Office doors and keys and access codes must always be kept secure, and keys and access codes must not be given to any third party at any time. If a staff member loses their office keys, they must report this to the Corporate Services Officer and Concierge Station without delay.

8.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by (e.g. through ground floor windows). If this cannot be avoided, then blinds should always be positioned to prevent this.

8.3 The receptionist is responsible for ensuring visitors sign in at reception. Visitors must always be accompanied and never left alone in areas where they could have access to confidential information. Visitors are the responsibility of the staff member(s) they are visiting.

8.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains our information, then steps should be taken to ensure that no confidential information is visible.

8.5 At the end of each day, or when desks are unoccupied, documents and devices containing confidential information must be securely locked away.

9 Computers and IT

9.1 Password protection and encryption must be used, where available, on our systems to maintain confidentiality.

9.2 Access to any computer or IT system will be secured by user ID and password. Passwords will contain a mixture of both upper- and lower-case letters, numbers and symbols and be of at least 8 characters in length). Passwords will be changed, at least, every 90 days. Passwords must not be written down in places where they are visible or shared with others.

9.3 Computers and other electronic devices must be locked when not in use and when staff leave their desks, to minimise the risk of accidental loss or disclosure.

9.4 Confidential information must not be copied onto portable media without the express authorisation of the Director. Information held on any of these devices should be transferred to the document management system as soon as possible for it to be backed up and then deleted from the device.

9.5 Staff must ensure they do not introduce viruses or malicious code on to our systems. Software must not be installed or downloaded from the internet without it first being virus checked and explicitly approved by the Corporate Services Officer. Staff should contact WWHC's Managed Service Provider (MSP) for authorisation and guidance on appropriate steps to be taken to ensure compliance.

9.6 WWHC's computer systems will be protected by malware protection software that is:

9.6.1 Licensed to WWHC

9.6.2 Paid for and not available without charge; and

9.6.3 Updated at least every 7 days.

10 Data Backup

10.1 WWHC data and email will be backed up daily and will not be changed or altered once created.

10.2 In addition, WWHC will store backup information:

10.2.1 in a manner that ensures all essential information relating to our business and software can be quickly and easily recovered.

10.2.2 away from the premises where the original data and software is held; and

10.2.3 take precautions to ensure that all data is stored safely.

10.3 WWHC will also ensure that equipment and data within the Concierge station pertinent to the door entry equipment will be backed up, at least, monthly.

11 Disposal of Computers, IT Equipment and Information

11.1 IT equipment (which includes its storage media) will be disposed of at the end of its useful life. Such equipment may store business information, confidential information and personal data and must therefore be disposed of in a secure manner to protect such information and to ensure that it cannot be accessed post disposal.

11.2 Prior to disposal, consideration should be given to whether it is possible to re-use IT equipment within the organisation, wherever possible.

11.3 If re-use is not possible, then the IT equipment must be disposed of via our contractor, who will remove the IT equipment from our office and issue a certificate to us to confirm that it has been disposed of securely and that all storage media have been wiped and destroyed. Secure disposal means that the IT equipment is destroyed in a manner that maintains the security of the IT equipment up to the point of destruction. We will only use contractors who provide sufficient guarantees in these regards.

11.4 Certificates of secure destruction provided by the contractor will be retained.

11.5 Staff must not attempt to wipe storage media themselves, as deleting a file does not permanently delete it and put it beyond use.

11.6 If staff have access to WWHC IT equipment at home or use portable devices as part of their roles, then such IT equipment must be returned to WWHC for disposal and must not be retained by staff or otherwise disposed of in domestic recycling or dump facilities.

11.7 The organisation will maintain an IT disposal register, recording details of the IT equipment that has been disposed of by the organisation (and the method of destruction), together with copies of the certificates issued by our contractor under paragraph 10.3. The Corporate Services Officer will maintain the IT disposal register.

11.8 Information containing business or confidential information or personal data must be disposed of using the confidential waste bins situated through the main office. These bins will be collected and disposed of by a third-party specialist contractor.

12 Communications and Transfer of Information

12.1 Staff must be careful about maintaining confidentiality when speaking in public places. This includes when working at reception, at home or when using public transport.

12.2 Confidential information must be marked "confidential" and circulated only to those who need to know the information during their work for the organisation.

12.3 Confidential information must not be removed from our offices, unless required for authorised business purposes, and then only in accordance with paragraph 11.4 below.

12.4 Where confidential information is permitted to be removed from our offices, all reasonable steps must be taken to ensure that the integrity and confidentiality of the information are maintained. Staff must ensure that confidential information is:

12.4.1 stored on an encrypted device, which has been authorised by the Corporate Services Officer, with strong password protection, and which is kept locked when not in use.

12.4.2 when in paper format, not transported in clear or other unsecured bags or cases.

12.4.3 not read in public places (e.g. waiting rooms, cafes and on public transport); and

12.4.4 not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots and cafes).

12.5 Postal and e-mail addresses and telephone numbers should be checked and verified before information is sent to them. Care should be taken with e-mail addresses to ensure that Microsoft Outlook auto-complete features have not inserted incorrect addresses.

12.6 All sensitive or particularly confidential information should be encrypted or password protected before being sent by e-mail or be sent by recorded delivery and its delivery tracked.

13 Personal E-mail and Cloud Storage Accounts

13.1 Personal e-mail accounts, such as Yahoo, Google or Hotmail and cloud storage services, such as Dropbox, iCloud and OneDrive, are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

13.2 Staff must not use a personal e-mail account or cloud storage account for our business purposes.

13.3 If staff need to transfer a large amount of personal data, they should contact the IT service provider for assistance.

14 Home Working

14.1 Staff must not take our information home unless required for authorised business purposes, and then only in accordance with paragraph 13.2 below.

14.2 Where staff are permitted to take our information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

14.2.1 personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by household members or visitors; and

14.2.2 all personal and confidential information must be returned to and disposed of at the office and not in domestic waste or at public recycling facilities.

14.3 Staff must not store confidential information on their home computers and devices.

15 Transfer to Third Parties

15.1 Third parties should be used to process our information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be “processors” for the purposes of data protection legislation. Examples of processers include our contractors, consultants and professional advisers.

15.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

16 Training

16.1 All staff will receive training on information security and confidentiality.

16.2 New staff will receive training as part of the induction process or upon return as periods of long-term absence. Further training will be provided on a regular basis or whenever there is a substantial change in the law or our policy and procedure.

16.3 Training is provided by the DPO, and attendance is compulsory for all staff at all levels. Training may be delivered online or in-person.

17 Reporting breaches

17.1 All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:

17.1.1 investigate the failure and take remedial steps, if necessary.

17.1.2 maintain a register of compliance failures; and

17.1.3 make any applicable notifications to the Information Commissioner's Office, the Scottish Housing Regulator and affected data subjects, if necessary.

17.2 Reference should be made to our Data Breach Management Procedure for our reporting procedure.

18 Consequences of Failure to Comply with this Policy

18.1 WWHC take compliance with this Policy very seriously. Failure to comply with it puts the organisations and its stakeholders at significant risk.

18.2 Due to the importance of this Policy, failure to comply with any requirement of it will be investigated and actioned in line with the Disciplinary and Grievance Policy. If an external organisation breaches this Policy, they may have their contract terminated by us with immediate effect.

18.3 Any questions or concerns about this Policy should be directed to the DPO.

19 Equalities

19.1 We are committed to ensuring equal opportunities and fair treatment for all people in our work. In implementing this Policy, we will provide a fair and equal service to all people, irrespective of factors such as gender, race, disability, age, sexual orientation, language or social origin or other personal attributes.

20 Policy Review

20.1 We will review and update this Policy in accordance with our data protection obligations, and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation or business operations.

Appendix 1 – Inventory of Information Assets

Organisational Unit	**Asset**	**Description**	**Purpose**	**Location**	**Asset Owner**	**Access**
Human Resources & Payroll	Employee data	Personal contact details, health information, financial, training, disciplinary, and contractual.	Information we are legally required to hold about an employee. Information we need to pay an employee and to manage their health and safety at work.	Paper copies in locked filing cabinet, electronic copies in restricted access folder on shared network drive. Clocking and attendance system accessed via logins.	Directorate Corporate Services Officer	Line Managers and Directorate. Staff in accordance with their rights. Finance and Corporate Services Officer for payroll purposes.
Corporate Services	Share Register	Register of all tenant members	Governance requirement.	Paper copies in finance cupboard, electronic copies on network drive,	Corporate Services Officer	All staff, Governing Bodies, Member or another eligible person(s)

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
				employee mail trays, HomeMaster		
Corporate Services	Accounts	Company financial and management accounts	Legal requirement	Electronic copies stored on shared network drive, Information published on WWHC website	Director, Deputy Director, Finance Officer	Public
Corporate Services	Accident Book	Log of employee accidents and near misses	Legal requirement	Paper copy in locked filing cabinet	Health & Safety Administrators	Line Managers, Health & Safety Administrators
Property Services	SHQS data	Property condition scores	Business requirement	Electronic, stored on shared network drive, HomeMaster	Property Manager	Internal

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
Property / Housing Services	Rechargeable Repairs	includes invoices to tenants, records of payment, debt collection info	Business requirement	Shared network drive and paper copies, HomeMaster	Housing Manager	Property & Housing Services staff
Property Services	Maintenance Register	log of all maintenance carried out to business and residential properties	Business requirement	Shared network drive, paper copies in Property section filing cabinets, HomeMaster	Property Manager	All staff
Housing Services	Tenant data	personal data including ethnic origin, disability, potentially violent	Business requirement	Shared network drive, paper copies in filing cabinets in hall, Customer engagement tool(s),	Housing Manager	All staff

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
				HomeMaster		
Housing Services	Occupant data	personal data including ethnic origin, disability, potentially violent	Business requirement	Shared network drive, paper copies in filing cabinets in hall, HomeMaster	Housing Manager	All staff
Housing Services	Tenancy data	Financial and estate management info include ASB, tenancy infringements, court action	Business requirement	Shared network drive, paper copies in filing cabinets in hall, HomeMaster	Housing Manager	Senior staff, Housing Services staff
Housing Services	Applicant data	personal data including ethnic origin, disability, potentially	Business requirement	Shared network drive, paper copies in filing	Housing Manager	Senior staff, Housing Services staff

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
		violent		cabinets in Housing Management office, HomeMaster		
Whitcomm	Customer data	Personal data including contact details, records of payment, payment references, debt collection info, invoices and statements.	Business requirement, Minute of Agreement	Accounting software accessed via secure logins, Shared network drive – restricted access protocols in place, paper copies in filing cabinets in Corporate Services Office	Corporate Services Officer	Corporate Services staff

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
Whitcomm	Financial data	Company financial and management accounts, banking and payment information, invoices, contracts and supplier information.	Business requirement, Minute of Agreement	Accounting software accessed via secure logins, Shared network drive – restricted access protocols in place	Deputy Director, Corporate Services Officer, Finance Officer	Deputy Director, Corporate Services Officer, Finance Officer, Whitcomm Committee
Concierge Station	CCTV	Images and video captured by estate-wide CCTV	Health & Safety, Security	GDX system in station, burnable and removable CD's	Concierge Manager	Directorate, Concierge staff, Housing Services staff, Public bodies
Concierge Station	Tenant data	personal data including ethnic origin, disability, potentially violent	Business requirement, Health & Safety	Paper copies & Concierge PCs in Concierge Station	Concierge Manager	Concierge staff, Housing Services staff

Organisational Unit	Asset	Description	Purpose	Location	Asset Owner	Access
Concierge Station	Housing Alarm information	Personal data including disability and emergency contact information	Business requirement, Health & Safety	Paper copies & Concierge PCs in Concierge Station	Concierge Manager	Concierge staff, Housing Services staff
WCRC	Tenant data	Personal data including contact information Data relating to tenant personal or financial circumstances.	Business requirement, tenancy sustainment and support, wider action	Staff laptops and emails secured with personal logins / PINs	Community Development Co-ordinator	All WWHC and WCRC staff

Equalities Impact Assessment

Policy/Project/Service Information			
Lead Officer	Corporate Services Officer		
Policy / Project / Service	Information Security Policy	**New Policy / Project / Service or revision of existing?**	Revision of existing – ISMS and ICT Disposal
Is this a reassessment following amendments being required at a previous assessment?	No		
Briefly describe the aims, objectives and purpose of the policy / project / service.	To ensure that all written, spoken and electronic information held, used or transmitted by or on our behalf, in whatever media is protected in the with GDPR legislation.		
Who is intended to benefit from the policy / project / service? (E.g. applicants, tenants, staff, contractors)	All WWHC stakeholders		
What outcomes are wanted from this policy / project / service? (E.g. the measurable changes or benefits to members/ tenants / staff)	To safeguard WWHC data (both physical and digital) from data breach, improper use, unauthorised access and that no stakeholders are adversely affected by WWHC actions.		

Consultation
Who have you engaged and consulted with as part of your assessment? N/A

Equalities Impact Assessment			
Which protected characteristics could be affected by the policy, practice, or service?		**Identify any positive impact/s that could result for each of the protected characteristic groups.**	**Identify any negative impact/s that could result for each of the protected characteristic groups.**
Age			N/A - Policy impacts groups of stakeholders rather than groups of protected characteristics
Disability			
Gender Reassignment			
Marriage & Civil Partnership			
Race			
Religion/Belief			
Pregnancy/Maternity			
Sex			
Sexual Orientation			

Action Plan To Mitigate Negative Impact		
What action/s are required to address the impacts arising from this assessment?		
Protected characteristics	**Action**	**Implementation Date**
Age		
Disability		
Gender Reassignment		

Marriage & Civil Partnership		
Race		
Religion/Belief		
Pregnancy/Maternity		
Sex		
Sexual Orientation		
Human Rights		

Final Decision	**Tick relevant box**	**Include explanation where appropriate**
Approved for implementation without change		
Amend or change the Policy/Project/Service		
Continue the Policy/Project/Service without change (despite impact)		
Stop the Policy/Project/Service		
Lead Officer Signature	R.Hosie	
Date	11/03/2026	
Date approved by Management Committee/ Sub Committee	30/03/2026	