West Whitlawburn
Housing Co-operative

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 Management System**
Policy Author	**Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**Apr 2024**
Latest date of Next Review	**Apr 2026**

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) is committed to preserving the confidentiality, integrity and availability of all the information held by the organisation. This Information Security Management System (ISMS) illustrates the reasons why WWHC require to protect the organisations information and outlines the procedures and policies in place to do so.

1.2 An ISMS is a set of policies and procedures for systematically managing an organisation's sensitive data. The goal of an ISMS is to minimise risk and to ensure business continuity by pro-actively limiting the impact of a security breach.

1.3 WWHC is a responsible organisation and having an ISMS will support our governance structure and helps to maintain the security of all business and personal information.

1.4 This policy supplements other policies and procedures implemented by WWHC and aims to comply with all legal and regulatory standards and improve our overall information security.

2. Legislation and International Standards

2.1 It is a legal requirement that WWHC processes data correctly; WWHC must collect, handle and store personal information in accordance with the relevant legislation and best practice:

2.1.1.1 The Data Protection Act 2018 (implements General Data Protection Regulation (GDPR));
2.1.1.2 The Privacy and Electronic Communications (EC Directive) Regulations 2003; and
2.1.1.3 ‘ISO 27001’ an internationally agreed standard that specifies the requirements for an ISMS.

3. Definitions

For the purposes of this policy the following definitions are used:

Business	Information that is collected, stored,

Information

processed or otherwise used by WWHC to provide services and carry out normal business functions. Includes information relating to housing applicants, current and former tenants, residents, current and former employees, contractors, suppliers, local authorities and regulators, solicitors, members, elected members, complainants and other service users.

Confidential

Information that is not made available to or disclosed to unauthorised individuals or entities.

Available

Information that is made available to and can be accessed by an authorised person as and when required.

Information Asset

Information that is valuable to WWHC (either financial, intellectual or reputational). It includes physical and digital information.

Personal Data

Information that helps to identify a living individual (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data

Information that relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation.

Data Protection Officer (DPO)

The member of staff responsible for monitoring WWHC’s compliance with Data

Protection laws and other related policies, co-operating with and serving as WWHC's contact for discussions with the ICO and reporting breaches or suspected breaches to the ICO and data subjects.

4. Scope

4.1 This policy relates to all business information and information assets that are collected, stored, processed or otherwise used by WWHC. It covers all WWHC information located (physically or digitally) within the main office building and Concierge station.

4.2 It further considers information that is held or used by one staff member located in Whitlawburn Community Resource Centre (WCRC) as well as data stored by WWHC on behalf of Whitcomm Co-operative Ltd as outlined in the *Whitcomm Service Costs and Minute of Agreement*.

4.3 The information covered by this policy includes all written, spoken, and electronic information, stored, used or transmitted by or on our behalf, in whatever media as well as information held on computer applications.

4.4 This policy applies to all staff, volunteers, committee and contractors or other agencies working on behalf of WWHC.

5. Purpose

5.1 The purpose of this policy is to ensure the integrity and security of all WWHC data. It is also implemented to ensure that WWHC fulfils its legal obligations as well as its mission and objectives outlined in the Business Plan 2023-2028.

5.2 In line with its vision and values, the Co-operative is also committee to upholding its reputation and protecting stakeholder data to ensure the highest standards of service. This policy aims to achieve this.

6. Risk Analysis and Management

6.1 WWHC understands that robust risk management is an integral part of its future planning both at strategic and operational levels and a key element of effective governance. It is also an important aspect of WWHC's decision making process.

6.2 WWHC's risk appetite is set out in the Risk Management Policy and Strategy. In summary, low, medium low, and medium risks are acceptable.

6.3 Senior staff conduct a risk analysis exercise on a quarterly basis which is reported to the Performance, Assurance and Risk Sub Committee. The document identifies and monitors risks and their likelihood and includes control measures put in place to reduce the risk or remove them completely.

7. Roles and Responsibilities

7.1 The Management Committee has overall responsibility for the information security management system with day-to-day responsibility being delegated to the Director.

7.2 Whilst all staff have the responsibility of ensuring information security, the following information assets are delegated to specific staff members in line with the current temporary structure:

Line Managers and Directorate	Human Resources , Personnel files and Recruitment
Finance Officer and Corporate Services Officer	Payroll Administration (in conjunction with line managers)
Finance Officer	Financial, Contracts and Audits
Corporate Services Officer	Time clocking and attendance systems, Governance, Health and Safety, IT management and security, Insurance, Audit
Head of Housing	Applicant, Tenant, Tenancy, Rent

Services	
Property Manager	Properties, Maintenance Contracts, Development Contracts, Gas Servicing, Compliance Information and Registers
Concierge Manager	CCTV, GDX system, Housing Alarms, Tenant and Tenancy
Community Development Co-ordinator	Wider action activities and projects, funding applications, case studies
Corporate Services Officer and Deputy Director	All Whitcomm Customer, Financial, Technical and Insurance data

7.3 Access to Information and Offices

7.3.1 All staff will be provided with a work email address and account and access to PC's and other IT applications, if required, as part of their role. Staff must ensure that such accounts are secured with password or PIN protection and locked when not in use. Staff must also ensure that any data received or transmitted using these systems is legitimate, accurate and traceable.

7.3.2 All office based staff are provided with a set of office keys and controlled door entry fob in which must be kept safe at all times. The concierge station holds a set of office keys for emergency call out circumstances (e.g. alarm activations). Should staff misplace or lose their keys they must notify their line manager immediately who should notify Concierge staff and the Corporate Services Officer.

7.3.3 The receptionist must ensure that visitors sign-in using the visitor log book at reception upon arrival at the office. They must always be accompanied by the staff member they are visiting and never left alone in areas where they could have access to confidential information.

7.3.4 Tenant access to office space (e.g. main office, Concierge station and WCRC) is restricted solely to the public reception(s) and interview rooms. Staff should make every effort to ensure that no unauthorised access is provided to office spaces where business information is stored. Physical barriers are in place to support this and should be used correctly at all times.

7.4 Financial Information

7.4.1 WWHC restricts access to financial information to specific members of staff. All roles and responsibilities are as indicated in the Financial Regulations policy. For the purposes of this policy;

access to the safe is restricted to the:

- Finance Officer
- Corporate Services Officer
- Finance Assistant
- Director
- Deputy Director
- Head of Housing Services
- Property Manager

Access to internet banking platforms is restricted to the:

- Finance Officer;
- Finance Assistant;
- Corporate Services Officer; and
- Deputy Director

7.5 Personal Information

7.5.1 All personal information will be processed in accordance with legislation as stated in section 2 of this policy as well as all other relevant WWHC policies and procedures.

7.5.2 WWHC will take all technical and organisational measures possible to ensure that personal information is secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

7.5.3 Staff may ask to review their personnel file and any other personal information in accordance with their rights under data protection legislation. Further information is contained in our

Privacy Policy.

7.5.4 Personal information will be kept for no longer than is necessary and stored and destroyed in accordance with our Privacy Policy.

7.6 Computers, IT and other Electronic Equipment

7.6.1 All staff are required to follow and acknowledge the terms outlined in the Computer Use Policy. Staff are required to ensure the safe storage of all mobile phones, laptops, tablets and all other portable digital media.

7.6.2 WWHC servers are located in the main office building. Access to the server cupboard is restricted solely to the Corporate Services Officer and Deputy Director. Other IT equipment is located within the Concierge station and access is restricted to Concierge staff and contractors with valid work orders and maintenance contracts.

7.6.3 WWHC's Managed Service Provider (MSP) manage the day-to-day IT function. The MSP has remote access to all WWHC main office IT equipment and PC's located within the Concierge station. The MSP will have access to the server cupboard when carrying out on-site works as instructed by the Corporate Services Officer or Deputy Director.

7.6.4 Upon termination of contract, staff must return all WWHC owned devices (e.g. mobile phones, laptops etc.) to the organisation. Staff email accounts will be retained for a 6 week period after their final working day. After this period the account will be deleted by WWHC's MSP as instructed by the Corporate Services Officer or the Deputy Director.

7.7 Disposal of information and IT Equipment

7.7.1 Information will be retained and disposed of in line with WWHC's Privacy Policy '*Table of Duration of Retention of certain Data – Appendix 5*'. Staff should make every effort not to delete or dispose of data that is required to be kept as part of our service delivery and contractual or legal obligations.

7.7.2 When disposing of paper copies of information (including business information and sensitive personal data) staff must use the confidential waste bins that are located throughout the main office. These bins will be collected and disposed of by a third-party.

7.7.3 IT equipment will disposed of in line with WWHC's Disposal of IT Equipment policy. An IT disposal register will be maintained by Corporate Services staff who will also instruct the disposal of all IT equipment with a credible supplier together with disposal certification.

7.7.4 Prior to disposal, consideration should be given to whether or not IT equipment can be re-used within the organisation. If this is not the case, the equipment should be recycled to promote the organisations Sustainability policy.

8. Communications and Transfer of Information

8.1 Staff must ensure to maintain confidentiality when working in public spaces. This includes when working at reception, at home or when using public transport.

8.2 Personal (including sensitive) and confidential information must not be removed from any WWHC site, unless required for business purposes, with prior consent from the employee's Line Manager and then only in accordance with section 8.4 below.

8.3 Where this information is permitted to be removed from a WWHC site, reasonable steps must be taken to ensure that the integrity and confidentiality of the information is maintained.

8.4 Staff must ensure that personal and confidential information is:

- stored on an encrypted device with strong password protection, which is kept locked when not in use;
- when in paper format, not transported in clear or other unsecured bags or cases, or disposed of using the staff members domestic waste or refuse facilities;
- not read in public places (e.g. public transport); and
- not left unattended in any place where it is at risk (e.g. in

conference rooms, car boots and cafes).

8.5 Staff must continue to implement WWHC’s Privacy, Computer Use and Homeworking policies when working off-site.

8.6 Postal and e-mail addresses, telephone numbers and bank account information should be checked and verified before information or funds are sent to them. If a staff member is in doubt about the information provided, they must verify the details with the recipient by method of telephone, in-person or in writing. All bank account information must be verified in writing.

9. Information Classification and Controls

9.1 Information assets are listed in Appendix 1 of this policy. Assets have been grouped by their location. They share the same vulnerabilities because they share the same physical and digital locations. Controls are in place to ensure the safety and integrity of assets.

10. Awareness and Training

10.1 All staff will receive training on information security, confidentiality and IT security.

10.2 New staff will receive training as part of the induction process or upon their return after periods of long-term absence. Further training will be provided on a regular basis or whenever there is a change in legislation, best practice or our policy and procedure.

10.3 Staff can request or be administered refresher training at any time should they or their line manager deem it necessary.

10.4 Training may be delivered online or in-person. Staff should make every effort to attend and engage in all training.

11. Reporting Breaches

11.1 WWHC understand that the mishandling of information can have a negative impact on its tenants, members and service users, employees, suppliers and other stakeholders and aims to ensure the integrity of all information at all times.

11.2 It further recognises that information breaches can happen and have implemented policies and procedures to ensure that the effect on individuals or the organisation is minimised and that remedial steps are taken.

11.3 All staff have an obligation to report actual or potential breaches to their line manager and the DPO who will decide if the breach requires to be reported to individuals or external agencies. Actual or potential breaches should be managed and reported in line with WWHC’s Protocol for Dealing with an Alleged Breach policy and it’s Privacy Policy.

11.4 Every breach will be logged and its cause, effect and treatment will be documented for reporting.

11.5 Senior Staff will monitor data breaches on a monthly basis. Cases that are common or consistent in nature must be investigated and changes to procedure or additional training arranged accordingly.

12. Equalities

12.1 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.

13. Policy Review

13.1 This policy will be reviewed every 2 years. Reviews may take place sooner according to changes in legislation or business operations.

14. Related Policies

The following policies must be read in conjunction with this policy:

- Business Plan 2023 – 2028
- Computer Use Policy

- Disposal of IT Equipment
- Financial Regulations
- Staff Code of Conduct
- Privacy Policy
- Protocol for Dealing with an Alleged Breach
- Risk Management Policy and Strategy
- Sustainability Policy

Appendix 1 - Inventory of information assets

Organisational Unit	**Asset ID**	**Asset**	**Description**	**Purpose**	**Location**	**Asset Owner**	**Access**
Human Resources & Payroll	A1.1	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	A1.2	Share Register	Register of all tenant members	Governance requirement.	Paper copies in finance cupboard, electronic copies on network drive, employee	Corporate Services Officer	All staff, Governing Bodies, Member or other eligible person(s)

					mail trays, HomeMaster		
Corporate Services	A1.3	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	A1.4	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	A2.1	SHQS data	Property condition scores	Business requirement	Electronic, stored on shared network drive, HomeMaster	Property Manager	Internal

Property Services	A2.2	Rechargeable Repairs	includes invoices to tenants, records of payment, debt collection info	Business requirement	Shared network drive and paper copies, HomeMaster	Property Assistant	Property Services staff
Property Services	A2.3	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	A3.1	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), HomeMaster	Head of Housing Services	All staff

Housing Services	A3.2	Occupant data	personal data including ethnic origin, disability, potentially violent	Business requirement	Shared network drive, paper copies in filing cabinets in hall, HomeMaster	Head of Housing Services	All staff
Housing Services	A3.3	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	Head of Housing Services	Senior staff, Housing Services staff
Housing Services	A3.4	Applicant data	personal data including ethnic origin, disability, potentially violent	Business requirement	Shared network drive, paper copies in filing cabinets in Housing Management office, HomeMaster	Head of Housing Services	Senior staff, Housing Services staff

Whitcomm	A4.1	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
Whitcomm	A4.2	Financial data	Company financial and management accounts, banking and payment information, invoices, contracts and	Business requirement, Minute of Agreement	Accounting software accessed via secure logins, Shared network drive – restricted access	Deputy Director, Corporate Services Officer, Finance Officer	Deputy Director, Corporate Services Officer, Finance Officer, Whitcomm Committee

			supplier information.		protocols in place		
Concierge Station	A5.1	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	A5.2	Tenant data	personal data including ethnic origin, disability, potentially violent	Business requirement, Health & Safety	Paper copies & Concierge PC's in Concierge Station	Concierge Manager	Concierge staff, Housing Services staff
Concierge Station	A5.3	Housing Alarm information	Personal data including disability and emergency contact information	Business requirement, Health & Safety	Paper copies & Concierge PC's in Concierge Station	Concierge Manager	Concierge staff, Housing Services staff
WCRC	A6.1	Tenant data	Personal data including contact information Data relating to tenant	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

			personal or financial circumstances.				

West Whitlawburn Housing Co-operative
Equality Impact Assessment

Name of Policy to be assessed	Information security Management Systems	**New policy or revision of existing?**	Revision/reformat of existing
Person(s) responsible for assessment		Corporate Services Officer	
Briefly describe the aims, objectives and purpose of the policy.	The aim of the Policy are to maintain the security and integrity of all WWHC data. The goal of an ISMS is to minimise risk and to ensure business continuity by pro-actively limiting the impact of a security breach.		
Who is intended to benefit from the policy? (EG applicants, tenants, staff, contractors)	Staff, tenants, members, applicants, contractors, all other stakeholders. WWHC Management Committee and the organisations reputation.		
What outcomes are wanted from this policy? (EG the measurable changes or benefits to members/ tenants / staff)	To ensure the security of all WWHC owned or processed data. To ensure security to all employees, tenants, members, applicants, contractors and other stakeholders personal and sensitive data. To ensure that WWHC is a responsible organisation and is compliant with all aspects of relevant legislation.		
Which groups could be affected by the policy? (note all that apply)			
Race		**Gender**	
Sexual orientation		**Gender reassignment**	
Age		**Religion or belief**	
Marital status		**Disability**	
Pregnant and Maternity			
If the policy is not relevant to any of the equality groups listed above, state why and end the process here.			
Policy impacts groups of stakeholders rather than groups of protected characteristics. Policies and other information can be provided in different formats upon request.			
Have those affected by the policy / decision been involved?			

Describe the likely positive or negative impact(s) that the policy could have on the groups identified above.	**Positive Impact(s)**	**Negative Impact(s)**
What actions are required to address the impacts arising from this assessment? (This might include: additional data, putting monitoring in place, making adjustments, taking specific action to mitigate any potentially negative impacts)		

Signed: Rachel Hosie

Job Title: Corporate Services Officer

Date: 18/04/2024