Caledonia
HOUSING ASSOCIATION

Cordale
HOUSING ASSOCIATION

Group Information Security Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Director of Strategy and Innovation
Author:	Director of Strategy and Innovation
Version number:	2.1
Approved by Chief Executive on:	October 2020
Governing Body Approved:	October 2020
Effective from:	October 2020
Due for review on:	October 2023
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	N/A
Procedure implemented:	
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	
Training Completed:	
Posted on intranet:	Yes
Posted on website:	Yes
Publicity material issued:	No

This document can also be provided in large print, braille, audio or other non-written format, and in a variety of languages.

1. Introduction

The Caledonia Group ('the Group'), comprising of Caledonia and Cordale Housing Associations, is committed to protecting the security of its information and information systems. It is the Group's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

2. Information Security

Information is a vital asset both in terms of the management of our business activities and the delivery of our wide range of services. Across the Group, it takes many forms, including personal, property and business information; exists in a range of paper based and electronic formats; and is accessed through a variety of office based and mobile devices. This policy focuses on the way in which we will ensure the security of the information that we hold, use and manage. It forms a key element of the Group's wider information governance arrangements alongside our policies and procedures on data protection, freedom of information, information risk management and remote and mobile working. The policy also links to the Group's developing cyber security and homeworking arrangements and will inform our work on these. The key elements of the Group's approach to ensuring information security are set out in the policy and have been developed to incorporate with the following overarching principles:

Confidentiality – information will be protected from unauthorised access, use and disclosure from unauthorised individuals, organisations or processes.

Integrity – the accuracy and completeness and reliability of information assets will be safeguarded.

Availability – information will be accessible and usable by an authorised individual, organisation or process.

3. Policy Aim

The aim of this policy is to establish and maintain security arrangements that ensure the confidentiality, integrity and availability of information assets, systems, applications and networks owned and / or held by the Group. We will aim to achieve this by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and the Group's other information governance related policies.
- Describing the principles of security and explaining how they will be implemented by the Group.
- Implementing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities and understand the associated information risks.
- Creating and maintaining within the Group a level of awareness of the need for Information Security as an integral part of system design and our day to day business activities.
- Protecting information assets under the control of the organisation.
- Effectively using information technology to support our information security arrangements.
- Maintaining consistency with our other information governance policies and practices.
- Meeting all legal and regulatory requirements relating to information security.

4. Policy Scope

The Policy applies to all information assets and information systems that the Group holds and operates, regardless of the type of information, the format, and/or where the information is stored. Likewise, the policy provisions apply to all areas of the Group's business and service activities, our governing body and staff team members and all contractors and suppliers working on behalf of the Group.

5. Equal Opportunities

The Group is committed to fairness and equality for all regardless of race, ethnicity, nationality (Gypsies, Travellers and white minority groups are included within these definitions), gender, sexual orientation, marital status, disability, state of health, age, beliefs or religion, appearance, family circumstances or criminal convictions. The Group's key aim is to ensure that its policies and procedures do not create an unfair disadvantage for anyone, directly or indirectly.

6. Responsibilities

All governing body and staff team members within the Group have responsibility for complying with this policy when handling or processing information and/or accessing information systems. This also involves reporting any security incidents immediately.

The following roles have key areas of responsibility in respect of Information Security:

IT Systems Manager is responsible for:

- Managing information security for the Group
- Monitoring standards and advising on security issues
- Managing investigations of Security Incidents
- Providing advice, guidance and training on Information Security

The Governance Officer is responsible for:

- Investigating, recording and reporting information security incidents
- Providing advice, guidance and training on Information Security

As regards the Group's wider information governance arrangements, the Director of Finance and Governance and Governance Manager are responsible for the implementation and development of these across the Group. The Chief Executive has overall responsibility for information governance including ensuring that key risks to the organisation, including those relating to information, are effectively managed in line with legal and regulatory requirements.

7. Information Security Measures

The information security measures noted in this section of the policy detail the way in which we will ensure the security of the information that we hold, use and manage.

Physical and Environmental Security

- All Group ICT and network equipment will be physically secured with appropriate access control to ensure that only authorised personnel have access.
- All paper based files will be stored in locations within our offices that can only be accessed by relevant authorised Group personnel. A 'clear desk' approach will be adopted to paper based information by all staff team members when they are not present in an office location.
- Wherever practical and as determined by ICT Services, equipment must be sited in a suitable environment to prevent loss, damage, or compromise of service and interruption to organisational activities.
- All non-Group persons accessing Group premises will be provided with appropriate visitor ID or other agreed identification.
- Controls will be implemented to minimise the risk or potential threats to the physical equipment which include theft, fire, electrical interference or failure, chemical effects or environmental hazards.

Group team members will be required to adhere to specific guidance provided on home and mobile working, including the security measures to be adopted in home and mobile working environments.

Network Security

- The Group network will be protected by key controls:

    - Managed Firewalls
    - Managed Routers
    - Managed Switches
    - Intrusion Detection System (IDS)
    - Intrusion Prevention System (IPS)
    - Virtual Private Networks (VPNs)
    - Mail & Content Filtering
    - Anti-Virus (AV)
    - Access control lists via Active Directory (AD)
    - Forced log-off functions

These form a key part of the Group's wider cyber security arrangements where the deployment of these security measures will be monitored and managed by the ICT Team. These layers of protection and security controls protect the network from both internal and external threats.

Creating, Controlling and Managing User Accounts

- Written procedures for access control and passwords based on business and security requirements will be developed and implemented for all systems.
- Users will only have access to the systems they are authorised for. Access to information systems will be granted only when required to access relevant information and take into account access rights, associated privileges and be authorised in accordance with the system owners. Access to privileged accounts and sensitive areas will be restricted.
- Password procedures will contain requirements such as frequency of change, minimum length, and character types which will be utilised to regulate password storage for each system. This is managed via Group Policy as an integral part of Active Directory (AD).
- Users should have unique combinations of usernames and passwords and are responsible for any usage of their account. Users must keep their passwords and system passwords confidential.
- Local administrator accounts will not be disclosed to users. Changes to administrator accounts must only be carried out by authorised ICT Team members.
- The Group Remote & Mobile Working Policy and other specific homeworking guidance issued will apply to all situations relating to remote access to the Group network and systems.

Monitoring of System Access and Usage

- Access and use of ICT systems will be monitored in order to detect unauthorised information processing activities. Usage will be traceable and auditable to a specific entity, e.g. a person, a device or a specific system.
- The ICT Team will register substantial disruptions and irregularities of system operations, along with potential causes of the errors. Capacity, uptime and quality of the ICT systems and networks will be monitored in order to ensure reliable operation and availability.
- The Group retains the right to intercept and record any form of electronic communication made on Group systems to gain access to required business communication, monitoring standards of service, prevent or investigating criminal activities and investigate unauthorised and / or misuse of the ICT system.

- The Group will monitor the performance and integrity of all systems on a continual basis and may withdraw access to any system if abuse or misuse is identified.

External or Third Party Access to Group Assets

- External parties include customers, consultants, auditors, developers and suppliers. Assets include information (databases, data files, etc.), software, hardware (including removable media) and services. Access to assets by external parties will not normally be permitted. Any decision to so must involve a specific business purpose and be approved by the relevant service director and the ICT Systems Manager.
- No third party ICT or devices can be installed on the Group network or equipment without explicit consent from the ICT Team.
- Access to the Group network, servers, or information systems by third parties will be controlled. The access requirements of any third party will be risk assessed by the ICT Team in conjunction with the relevant Service
- Director, and access will not be granted until the outcome of this assessment is confirmed. Any regular access provided to third parties will have formal agreements or contracts in place.
- Third party accounts will be configured to automatically disable after the period defined in the agreement or contract.

Storing Information

- Users of the Groups PCs, laptops, tablets and mobile phones should always save data to a network shared drives. In future, shared drives will be replaced by an Electronic Document Management (EDM) solution, Microsoft Teams and SharePoint. Users are not permitted to save any data to any local storage.
- All paper based information must be securely stored in the appropriate files within the Group's office locations. This information should not be removed from the office locations unless approval is granted by the appropriate service manager and appropriate security controls agreed.

System Configuration and Device Security

- Changes to any network configuration will only be carried out by the ICT Team or the Group's approved third party support agency.
- The ICT Team will maintain documentation of physical and virtual servers, services hosted, protocol usage and available ports and related device configuration.
- All applications and access to the IT services and functionality will be controlled and securely managed by Active Directory (AD).
- All computers and servers connected to the Group network will run the latest version of the operating system and installed applications, have the latest available security patches and updates installed and have up to date anti-virus software enabled and configured to run weekly scans.
- Team members must notify the ICT Team immediately if they suspect their device has become infected or compromised in any way. Any service or system suspected of being infected will be isolated from the network immediately.
- All laptop devices will be encrypted using a recognised, industry standard Disk Encryption solution.
- All laptops will be managed using a Network Management and Control solution.
- All mobile devices (mobile phones and tablets) will be managed using the Group's Mobile Device Management (MDM) solution.

Backups and Recovery

- The ICT Team and third party Business Partners will ensure that adequate controls and procedures are in place for the regular backup and recovery of all information held and used by the Group.

- Back-up and recovery procedures will be documented and tested. Operation logs will be maintained and be subject to regular checks.

Data Encryption

- Storage and transfer of any data covered by defined by Data Protection legislation and sensitive Group information will be encrypted and/or password protected.

Disclosure of Information

- Any disclosure of Group information will be in accordance with the Group information governance policies.

Data and Hardware Disposal

- The ICT Team will ensure all electronic data will be removed from all devices prior to secure disposal. Where electronic data in our ICT systems requires to be deleted, this will be carried out line with the requirements of the Group Data Protection Policy.

8. Procurement of New Technology

Any procurement of new software or hardware must be approved by procured through the Group ICT Team. This will also include installation and usage and arrangements for using on, or accessing via, the Group's ICT network. The provisions of this policy will apply to all new software or hardware. Any new system that will involve the processing of personal data will be assessed using the Group's Data Protection Impact Assessment (DPIA) process.

9. Information Security Incident Management

All Information Security Incidents must be reported immediately to the IT Systems Manager and Governance Officer in accordance with the Security Incident and Breach Reporting Procedure. All incidents will be progressed in line with this procedure.

10. Acceptable Use / Internet and E-mail

The Group's Internet and email system are provided primarily to enable Group staff to better communicate with other members of staff and outside agencies. Occasional and incidental use of Internet and email for personal use is permitted as long as this does not interfere with the performance of duties, put either the user or the Group at risk or create any information and / or cyber security risks. The use of these systems will be monitored where required and excessive use of these facilities for purposes other than Group business may result in disciplinary action.

11. Training

All governing body and staff team members will be made aware of the provisions of this policy and good practice in information security. This will include briefings on information security as part of wider cyber security training. Role specific training will be provided for team members who have responsibility for managing information assets and systems to ensure they understand their roles when working with these.

12. Breach of Policy

Any breaches of this policy may be considered under the Group disciplinary procedures, and may result in disciplinary action being taken, including dismissal. Actual or suspected information security incidents should be reported immediately to the Governance Officer and ICT Services, as highlighted in the Security Incident and Breach Management Procedures.

13. Monitoring and Reporting

Regular audits will be undertaken to ensure compliance with the relevant legislation, this policy and any related information security procedures. Significant risks resulting from Information Security incidents will be recorded in the Corporate Risk Register which is reported regularly to the Executive Management Team and the Management Board. All procedures and guidance will be reviewed on a regular basis to ensure they meet regulatory requirements and best practice.

14. Policy Review

This policy will be reviewed every three years by the Group, although changes will be made to the policy during the three-year period if required to meet changes in legislation and regulation; to reflect any amendments made to the Group's other information governance or risk management policies; and to address any gaps in the policy that have been identified from an information risk incident.