Group Information Risk Management Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Director of Strategy and Innovation
Author:	Director of Strategy and Innovation
Version number:	1
Approved by Chief Executive on:	December 2020
Governing Body Approved:	December 2020
Effective from:	December 2020
Due for review on:	December 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:	
Posted on website:	
Publicity material issued:	

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

Group Information Risk Management Policy

1. Introduction

The Caledonia Group ('the Group'), comprising Caledonia and Cordale Housing Associations, recognises that the effective management of risk is a key factor in the successful delivery of our strategic aims. The Group's Risk Management Policy details our approach to managing risk across our organisation and business activities. Information risk management within the Group is an important governance and operational consideration within this approach.

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. It is also an asset that is subject to risks as regards the various legal and regulatory requirements that apply to information management and the threat of criminal activity including cyber-attacks, phishing scams and fraud.

This policy focuses specifically on the management of risk to information held and used by the Group and sets out our approach to this. It forms a key element of the Group's information governance framework alongside other linked policies. These policies are summarised in table below and in Appendix 1, with each relating to specific aspects of the Group's information management aims and responsibilities. An overview of the implementation of the Group's information governance policies in relation to key identified information management risks is provided in Appendix 2.

Group Information Governance Framework	
Risk Management	**Data Protection / GDPR**
Sets out the overall framework and approach for managing service and business risks across the Group	Sets out how we will comply with legislation relating to the collection, handling and protection of personal data and associated business information.
Information Risk Management	**Document Retention**
Identifies key risks to our information assets and details our specific approach to managing these risks and protecting the assets	Specifically details how information will be retained or disposed of to meet data protection requirements, including a retention schedule
Information Security (& Remote and Mobile Working)	**Freedom of Information & Environmental Information**
Details the various security measures we will deploy to ensure the confidentiality, integrity and security of our information assets	Sets out how we will comply with FOI and EIR legislation (information requests, advice & assistance and publication of information)

2. Scope and Policy Aims

This policy and its supporting processes and procedures apply to all information used within the Group. Likewise, the provisions of this policy apply to all areas of the Group's business and service activities, our governing body and staff team members and all contractors, suppliers and partner agencies working on behalf of the Group.

This policy sets out the Group's commitment to effectively manage information risks. We will aim to achieve this by:

- Maintaining consistency with our established risk management and information governance practices.
- Effectively identifying all information assets held by the Group and potential threats to these.
- Ensuring that risks relating to the confidentiality, integrity and availability of the Group's information are identified, assessed and managed with appropriate actions and controls.
- Creating a pro-active organisational culture where information is valued and information risk management is embedded within the design of our business processes and in our day to day service activities.
- Ensuring individuals with information management responsibilities are clear on these and understand the information risks associated with their operational function and how these could affect wider business sustainability and success.
- Safeguarding the Group's information assets and protecting as a far as possible our customers and governing body and staff team members from information risks.
- Managing, reviewing and reporting on information risks.
- Effectively using information technology to support our information risk arrangements.
- Meeting all legal and regulatory requirements relating to information risk management, including ensuring all governing body and staff team members are aware of these.

3. Roles and Responsibilities

Roles that have key areas of responsibility for information risk management within the Group are noted below. Summary information on these responsibilities in a RACI matrix format is also provided in Appendix 3.

Group Governing Bodies

The Caledonia Management Board and Cordale Management Committee collectively, and also through the work of the Audit and Risk Management Committee, are responsible for ensuring that the Group's risk management processes provide them with adequate assurance on the management of information risks and the associated legal and regulatory requirements.

Chief Executive

The Chief Executive has overall responsibility for risk management and information governance within the Caledonia Group, including ensuring that key risks to the organisation, such as those relating to information, are effectively managed in line with legal and regulatory requirements.

Director of Finance and Governance

The Director of Finance and Governance is responsible for overseeing the Group's risk management and information governance frameworks, and policy development relating to these. This includes ensuring that this policy and the identified risks are reviewed on a regular basis; reporting to the Group's governing bodies and Audit and Risk Management Committee on relevant information governance issues; and embedding an information risk management culture across the Group.

Governance Manager

The Governance Manager is responsible for the day to operational implementation of the risk management and information governance frameworks and the associated system development

activity. This includes the investigation of information risk security incidents, coordination of the review of the Group's information asset registers and the consistent implementation of information management contractual provisions by the Group's service teams.

ICT Systems Manager

The ICT Systems Manager is responsible for ensuring that the Group's ICT systems and working arrangements support the implementation of this policy and the achievement of the stated aims.

Service Directors and Managers

Service Directors and Team Managers are responsible for ensuring that the provisions of this policy are fully implemented in all aspects of the work carried out by their respective teams. This includes risk identification, management, review and reporting relating to the information management activities and assets within their teams; ensuring a consistent approach to this across the Group; assessing whether better use could be made of the information held; ensuring information management related provisions within service contracts are adhered to; and contributing to the development and review of the Group's information risk arrangements.

Everyone involved in the Group

Everyone who works for, or with, the Group will create, use or otherwise process information in the course of their work. They must therefore ensure that information is handled and managed in line with this policy and the Group's other information governance related policies. There is a key responsibility to report any breach or suspected breach of this policy to the immediate line manager and the Governance Manager for investigation.

Contractors, Suppliers and Partner Agencies

There are aspects of the Group's business functions that involve information assets being processed by contractors, suppliers and partner agencies on our behalf. The information risks that apply in these situations mirror those noted for the Group in Appendix 2. Given this, the same policy requirements will be applied on the same basis as if the functions were being managed directly the Group. This will involve requirements that relevant Group policies (or equivalent internal policies) are implemented as key contractual requirements. Data Protection Agreements will also be included as standard in service contracts, and then managed and reviewed by service teams in line with the Group's contract management arrangements. Furthermore, appropriate measures will be adopted to ensure that the installation, maintenance and development of software and associated equipment used by external parties providing services for the Group is secure, for clear business purposes only and does not affect the security of existing Group systems.

4. Organisational Context

Information is an important and valuable organisational asset for the Group. The Group's two housing associations provide a wide range of housing and related services to a diverse customer group across a wide geographical area. The delivery of these services involves the handling, processing and sharing of a wide range of information in a variety of different ways. Likewise, the Group's business management activities involve a diverse staff team who the use different types of information, including personal and also commercially sensitive information, in relation to a wide range of tasks.

The Group's existing information governance framework has a focus four specific areas – data protection, GDPR compliance, freedom of information requirements and information security relating to the Group's ICT systems and devices. Policy and procedure documents are in place for these and

detail the associated operational arrangements. In relation to data protection, this includes the appointment of a Group Data Protection Officer who has a key coordinating and advisory role on a range of data and information compliance issues, including the management of data breaches. The Group's risk management arrangements also include the assessment, management and review of the risks associated with our existing information governance framework. This policy had been developed to interlink with this framework.

The Group currently has in place a range of information asset registers that detail the type of information held and used by each of the directorate teams. These registers were developed specifically for the purposes of GDPR compliance and therefore have a specific focus on personal information. As part of the implementation of this policy, these registers will be reviewed and developed further to ensure that they incorporate all relevant personal and also business / commercial data held by the Group and can be used effectively to inform our information risk management activities. Processes will also be developed to ensure the asset registers are kept up to date and complete and that there is a clear link between these and our other information governance and business requirements.

5. Information Risk Management Approach

Information risk management involves assessing and mitigating the impact of risks to our information assets and systems. The Group is aware that these risks can never be eliminated fully but we also understand that information risks must be managed effectively and proportionately.

The Group Risk Management Policy sets out our approach to identifying, managing and reviewing key business risks and the potential impact that these may have on the Group's sustainability and success. The policy sets out a structured risk management process based on an ongoing cycle of review and the balancing of risk and control through appropriate actions. Risks are identified, assessed and measured in terms of likelihood and impact and prioritised in terms of an assessed risk score. Mitigation, management and control actions in relation to each specific risk are detailed.

Our information risk management approach will involve the implementation of this methodology and relating this also to the confidentiality, integrity and availability (defined below) of the information we are responsible for.

Confidentiality	The protection of information from unauthorised access, use and disclosure from unauthorised individuals, organisations or processes.
Integrity	The safeguarding of the accuracy and completeness and reliability of information assets.
Availability	Information being accessible and usable by an authorised individual, organisation or process.

A summary list of initial risks identified against these aspects, and an associated risk classification and mitigation review, and is provided in Appendix 2.

6. Risk Governance and Reporting

As noted in Section 3 above, the Group's Finance and Governance Director and Governance Manager are responsible for the development and implementation of the Group's information governance and risk management frameworks. In terms of this policy this responsibility includes:

- Ensuring clarity on the policy provisions and implementation requirements across the Group.
- Setting out appropriate information controls and management processes.
- Co-ordinating the regular reviews of the Group's information asset registers.
- Providing reports to the Group's governing bodies on the management of information risks.
- The regular review and re-assessment of the information governance risk map.
- Arranging regular information management audits to ensure compliance with legal and regulatory requirements, and to provide assurance for the Group's governing bodies.
- Reporting any significant information risk incidents to the Executive Management Team and the governing bodies.

7. Training

All governing body and staff team members will be made aware of the provisions of this policy and general accepted industry practice in relation to information risk management, and also where to find associated guidance and support. Learning programmes relating to information risks and cyber-security will be developed and implemented across the Group. The will also involve the mechanisms to assess the effectiveness of the associated training, with the outcomes used to determine and shape of future learning activity within the Group.

8. 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 risk security incidents should be reported immediately to the Group Data Protection Officer and ICT Services as highlighted in the Security Incident and Breach Management Procedures.

9. Equality and Diversity

The Group recognises the diversity of the communities where we work and our governing body and staff team members. We aim to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their needs. In line with this, the policy has been assessed for equality impact on the protected groups, as set out in the equalities legislation. Also, the Policy is applicable to all Group governing body and staff team members irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

10. Policy Review

This policy will be reviewed at least 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.

Appendix 1 – Summary Overview of Group Information Governance Policies

Policy	Information Management Focus	Applies To
Data Protection (including GDPR)	Sets out how the Group will comply with and implement all relevant data protection legislation relating to the collection, handling and protection of personal data. It details the steps that will be taken to collect, handle and store all personal data and associated business information in line with the data protection principles and rights of individuals set out in data protection legislation (including GDPR).	Governing bodies Staff team Contractors Suppliers Partner agencies
Group Document / Information Retention and Destruction Policy	Details a robust framework that governs how information / documentation is retained or disposed of within the Group in order to meet data protection legislation requirements. This also includes the Group's information retention schedule for different file / documents types. This policy directly links to the Data Protection policy.	Governing bodies Staff team Contractors Suppliers Partner agencies
Freedom of Information and Environmental Information	Sets out the provisions of Freedom of Information (FOI) legislation and Environmental Information Regulations (EIR) as they apply to the Group; and the approach the Group will take in complying with the associated requirements (responding to information requests, providing advice and assistance to individuals and the publication of information).	Governing bodies Staff team
Risk Management	Establishes the approach and framework to the management of risks across the Group's business and service management activities, and also sets out the Group's risk appetite. The risk management procedure detailed within this is used to guide the Group's specific consideration of risks relating to information management.	Governing bodies Staff team
Information Security	Details the way in which the Group will ensure the confidentiality, integrity and security of the information assets that we hold, use and manage, including protection against cyber-security threats. The various information security measures deployed are detailed. This includes those relating to physical security; network, device and data security; managing user accounts; system configuration, access and usage; and external / third party access to Group information assets; and data and hardware disposal.	Governing bodies Staff team Contractors Suppliers
Remote and Mobile Working	Sets out the security and business operations related requirements as regards the use of mobile computing devices and other computing devices which are not located on Group premises, including when these devices are used to access Group information assets and the Group network. The policy directly links to the Information Security Policy.	Governing bodies Staff team Contractors Suppliers

Appendix 2 – Overview of Group Information Management Risks

Policy Priority	Risk Issue	Risk Category	Prevention / Mitigation
Confidentiality	Cyber-security attacks leading to loss and / or misuse of Group information, resulting in legal and regulatory action, financial penalties, potential theft / fraud and reputational damage.	1. Compliance 2. Regulatory 3. Financial	Implementation of multi-layered approach to network, device, application and account security as detailed in the Information Security Policy – includes the measures to prevent unauthorised access, damage or interference to sensitive, confidential, business critical, personal information and/or documents. Cyber-security awareness programmes for the staff team on an annual basis. Procedural guides for team members.
	Unauthorised or accidental disclosure of Group information resulting in legal and regulatory action, financial penalties and reputational damage.	1. Compliance 2. Regulatory 3. Financial	Implementation of the Group's Policies on Data Protection, FOI, Information Security and Remote and Mobile Working. Information management, data protection and FOI awareness programmes for the staff team annually. Procedural guides for team members.
	Unauthorised or accidental disclosure of sensitive personal information resulting in data protection breaches, financial penalties and customer dissatisfaction.	1. Compliance 2. Regulatory 3. Operational	Implementation of the Group's Policies on Data Protection, FOI, Information Security and Remote and Mobile Working. Information management, data protection and FOI awareness programmes for the staff team annually. Procedural guides for team members
	Unauthorised disclosure of information by agencies acting on behalf of the Group resulting in legal action, financial penalties and reputational damage.	1. Compliance 2. Regulatory 3. Financial	Application of the relevant Group information governance policies to the agencies involved as key contract requirements. Data Protection Agreements included as standard in service contracts, and managed / reviewed in line with contract management arrangements in place. Review of security aspects of systems / software to be used.
	Inadequate electronic and physical protection of electronic and hard copy files resulting in data protection breaches, customer dissatisfaction, the release of commercially sensitive information, financial penalties, and reputational damage	1. Compliance 2. Regulatory 3. Financial	Physical and environmental security measures and network, device, data, application and account security arrangements implemented in line with the provisions of the Information Security Policy. Training and guidance provided for team members on information and data security issues.
Integrity	Inadequate information management discipline and practices resulting in inaccurate / incomplete / unreliable data,	1. Operational 2. Compliance 3. Regulatory	Information governance awareness programmes for the staff team annually. Procedural guides for team members on information governance tasks. EDMS system implementation. Coordination and

	poor decision making, service delivery problems, information security breaches and potential legal action.		oversight of information governance tasks across the Group by the Governance Team (with assistance from the Data Protection Officer (DPO) where required).
	Important business information is incorrectly disposed of resulting in potential regulatory action, service delivery failures and decision making problems.	1. Operational 2. Regulatory	Implementation of the provisions of the Group Document / Information Retention and Destruction Policy. Procedural guidance for the staff team. Document retention awareness training for the staff team on a regular basis. EDMS system implementation.
	New business systems and processes don't take information risk into account resulting in inaccurate / incomplete / unreliable data, poor decision making, business management and service delivery problems and potential legal and regulatory action.	1. Operational 2. Compliance 3. Regulatory	Information management assessments to be completed as part of the requirements specification document for any proposed new / updated business system. Advice to be provided by the ICT and Governance teams, with advice also from the DPO as required.
	Duplication of digital files and information in different IT systems, resulting in increased risks of security breaches, inefficient working arrangements and potential failures in meeting legal requirements (e.g. FOI and subject access requests).	1. Operational 2. Compliance	Regular review of the Group's information asset registers, co-ordinated by the Governance Team, to ensure the integrity of these; and the development of procedural guidance to support this activity and ensure the registers are kept up to date, accurate and complete and comply with all relevant information governance requirements. EDMS system implementation.
Availability	Failure to ensure information is available / communicated to the right people at the right time within the Group resulting in service delivery and business management problems, customer dissatisfaction, contractor issues and poor decision making.	1. Operational 2. Regulatory	Regular review of the Group's information asset registers, co-ordinated by the Governance Team, to ensure the integrity and availability of these meeting business and service requirements. Governance and ICT Teams will support operational teams with local information management responsibilities.
	Failure to comply with relevant legislation relating to information availability (e.g. Freedom of Information / GDPR) leading to legal and regulatory action, financial penalties, customer dissatisfaction and reputational damage.	1. Compliance 2. Regulatory	Information governance awareness programmes for the staff team annually. Procedural guides for team members on information governance tasks. Coordination and oversight of information governance tasks across the Group by the Governance Team (with assistance from the DPO where required).

Appendix 3 - Roles and Responsibilities - RACI Matrix

Key:

- R = Responsible – this role has responsibility for performing and completing the activity
- A = Accountable – this role takes the key decisions and actions on the activity
- C = Consulted – this role will be communicated with for feedback and views on the activity
- I = Informed – this role will be updated on decision and actions taken on the activity

Activity	Governing Body	CEO	Director F&G	Governance Manager	ICT Manager	Service Directors & Managers	Team Members	DPO*	Contractors Suppliers
Determine risk management approach	C	A	R	C	C	C	I	I	I
Implement risk management approach	I	C	A	R	C	C	I	I	I
Implement information risk framework	I	C	A	R	C	C	I	I	I
Assessment and reporting of information risks	I	C	A	R	C	C	I	I	I
Operational management of information risk framework	-	C	A	R	C	C	I	I	I
Co-ordination of information security incidents	I	C	A	R	C	C	I	C	I
Implementation of information risk ICT arrangements	-	C	A	C	R	C	I	I	I
Implementation of Information Risk Policy & procedures	-	C	A	R	C	C	I	I	I
Management of 3rd party information risks	-	C	A	R	C	C	I	C	I

*DPO (Data Protection Officer) service currently provided by Harper Macleod Solicitors