Group Data Protection Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Director of Finance & Governance
Author:	Governance Manager
Version number:	1.1
Approved by Chief Executive on:	15 May 2018
Governing Body Approved:	15 May 2018
Effective from:	16 May 2018
Updated:	October 2020
Due for review on:	15 May 2021
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	N/A
Procedure implemented:	Yes
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	Yes
Training Completed:	Yes
Posted on intranet:	Yes
Posted on website:	Yes
Publicity material issued:	Yes
Business Services – Implementation Review:	N/A

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

1 Introduction

1.1 The Caledonia Group ('the Group'), comprising Caledonia, Cordale and Bellsmyre Housing Associations, processes personal data about individuals in order to deliver our services. We process personal information to enable us to provide social housing accommodation and associated services, including:

- letting, renting and leasing properties
- carrying out research
- administering housing and property grants
- providing associated welfare services, advice and support
- maintaining our accounts and records
- supporting and managing our Governing Body, staff, agents, and contractors

1.2 The lawful and appropriate management of personal data is extremely important to the Group. Our ongoing success depends upon promoting transparency and maintaining the confidence of our customers and employees.

1.3 This policy sets out the Group's commitment to protecting personal data and how we will implement this with regards to the collection and handling of personal data as defined in the following legislation:

- General Data Protection Regulations (EU) 2016/679 (GDPR)
- UK Data Protection Bill which will replace the Data Protection Act 1998
- Privacy and Electronic Communications Regulations (PECR)
- Any related Information Security legislation
- Any legislation that will replace the GDPR in UK law after leaving the European Union.

1.4 Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

2 Scope

2.1 The Policy applies to all personal data that the Group holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual e.g. name, address, email, postcode, CCTV image, and photograph. Special categories of personal data are information about racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual health and trade union membership.

2.2 The policy applies to personal data held or accessed on the Group premises or accessed remotely via home or mobile working. Personal data stored on any removable devices is also covered by this policy.

2.3 This policy applies to:

- Governing Body Members
- Staff, including temporary staff
- Volunteers
- All contractors and suppliers working on behalf of the Group

3 The Data Protection Principles

3.1 Data Protection laws describe how organisations must collect, handle and store all personal data. Ensuring compliance is underpinned by the following principles.

Personal data must be:

3.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

3.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;

3.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

3.1.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 In addition to these principles the law requires organisations to be both responsible for and be able to demonstrate compliance with the above principles.

4 Responsibilities for Compliance

4.1 **Everyone** who works for, or with, the Group has a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in line with this policy and the data protection principles.

The following roles have key areas of responsibility:

4.2 **The Caledonia Management Board and the Chief Executive** are responsible for ensuring that the Group meets its legal obligations. The Management Committee for Cordale and Bellsmyre also have responsibility for ensuring legal obligations are met for the two respective organisations.

4.3 **Executive and Operational Management Team members** are responsible for ensuring that the provisions of the policy are fully implemented in all aspects of the work carried out by their respective teams.

4.4 **The** Governance Officers are responsible for:

- undertaking the role of Group Data Protection Officer
- being the main contact on Data Protection issues
- liaising with the ICO on all related matters
- informing and advising the Group and everyone who handles personal data on behalf of the Group of their obligations under the regulations
- monitoring compliance with the regulations

- providing advice on completing Privacy Impact Assessments
- supporting and managing data subjects' right of access
- recording and maintaining appropriate records of the Group's processing activities and compliance with the law
- managing personal data breaches

4.5 The **Group's Data Protection Officer** role is responsible for ensuring the Group's compliance with Data Protection Laws by:

- Monitoring compliance
- Providing advice and information to the organisation
- Providing direct support and advice to data subjects
- Managing security incidents and breach investigations
- Liaising with the ICO on behalf of the different Group data controllers

4.6 **IT Systems Manager** is responsible for:

- IT Security
- Relevant IT policies and procedures

4.7 **Group Data Controllers are** responsible for:

- Local implementation of Data Protection policies and procedures
- Liaising with the Data Protection Officer on all related issues

5 Processing Lawfully and Fairly

5.1 The Group will ensure processing of personal data, and special categories, meets the conditions as outlined in legislation. Individuals will be advised on reasons for processing via a freely available Privacy Notice.

5.2 Where data subjects' consent is required to process personal data, this consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

6 Purposes for Processing

6.1 Personal data will only be used for the original purpose it was collected for. These purposes will be made clear to all Data Subjects.

6.2 If the Group wish to use personal data for a different purpose than previously notified, we will notify the data subject prior to processing.

7 Adequate and Relevant data

7.1 The Group will only collect the minimum personal data required for the purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted.

7.2 Any personal information that is optional for individuals to provide will be clearly marked as such.

8 Accuracy of Data

8.1 The Group will take appropriate steps to keep personal data up to date, where relevant, to ensure accuracy and correct processing.

8.2 Any personal data found to be inaccurate will be updated immediately. Any inaccurate personal data that has been shared with third parties will also be updated.

9 Retention

9.1 The Group will hold data for the minimum time necessary to fulfil its purpose. Timescales for the retention of personal data will be outlined in the Group's Records Retention Schedule.

9.2 Data will be disposed of in a responsible way to ensure confidentiality and security.

10 Security

10.1 The Group will implement appropriate security measures to protect personal data.

10.2 Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis.

10.3 Employees will keep all data secure, by taking sensible precautions and following the Group IT Security Policy.

11 Data Sharing

11.1 In certain circumstances the Group will share personal data with third parties. This may be part of a regular exchange of data, data sharing from one part of the organisation to another or one-off disclosures in unexpected or emergency situations.

11.2 Appropriate security measures will be used when sharing any personal data.

11.3 Where data is shared regularly a contract or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

11.4 The Group will consider all the legal implications of sharing personal data prior to doing so.

11.5 Data Subjects will be advised of any data sharing in the Privacy Notice.

12 Data Processors

12.1 Where the Group engage Data Processors to process personal data on our behalf, the Group will ensure:

- Data processors have appropriate technical security measures in place;
- No sub-processors are used without prior written consent from the Group;
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

13 Security Incident & Breach Management

13.1 All security incidents or personal data breaches must be reported to and subsequently investigated and managed by the Data Protection Officer, under the Group Security Incident and Breach Management Procedures.

13.2 The Information Commissioner's Office, the individuals affected and any relevant third parties will be notified immediately, if required.

14 Individual Rights

14.1 The Group will uphold the rights of data subjects to access and retain control over their personal data held by us.

14.1.1 **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.

14.1.2 **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.

14.1.3 **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.

14.1.4 **Right to Erasure** (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.

14.1.5 **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.

14.1.6 **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine readable format.

14.1.7 **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

15 Privacy by Design

15.1 We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the Group.

15.2 When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out Data Privacy Impact Assessment.

16 Training

16.1 All staff, volunteers, and Governing Body members will be made aware of good practice in Data Protection and where to find guidance and support for data protection issues.

16.2 Adequate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities.

17 Breach of Policy

17.1 Any breaches of this policy may be considered under the Group disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

18 Monitoring and Reporting

18.1 Regular audits will be undertaken to check compliance with the law, this policy and any relevant procedures.

18.2 Severe risks resulting from data protection compliance requirements will be considered and monitored within the Group's risk management arrangements.

19 Related Policies & Procedures

19.1 The implementation of this policy will be supported by specific procedural guidance. This will be reviewed and developed on a regular basis to ensure ongoing compliance with legal, regulatory and good practice requirements.

20 Policy Review

20.1 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 or any associated requirement.