GROUP DATA PROTECTION POLICY

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Business Performance Manager
Author:	Business Performance Manager
Version number:	1.0
Approved by Chief Executive:	Yes
Approved by Caledonia Management Board on:	26 January 2016
Effective from (Caledonia HA):	January 2016
Approved by Cordale HA Committee of Management on:	19 January 2016
Effective from (Cordale HA):	January 2016
Due for review on:	January 2019
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	Yes
Procedure implemented:	Yes
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	
Training Completed:	
Posted on intranet:	February 2016
Posted on website:	February 2016
Publicity material issued:	
Business Services – Implementation Review:	

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

CONTENTS

1. Introduction to the Data Protection Act 1998

1.1 The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of an organisation to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

The Data Protection Act 1998 is underpinned by a set of eight principles with the legal duty for enforcing compliance with the Act falling to the Information Commissioner Office (ICO).

1.2 The Caledonia Group ('the Group'), comprising Caledonia and Cordale Housing Associations, is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998.

In order for Group members to operate effectively, they have to collect, and process information about a range of people including, but not limited to, the following:

- tenants;
- employees (past and current members of staff and applicants);
- housing applicants;
- sharing owners;
- Governing Body and Tenant Committee members; and
- contractors/suppliers.

In order for the Group members to comply with the law, information about individuals must be collected and used fairly, stored safely/securely and not disclosed to any third party unlawfully.

All processing of personal data (includes collection, holding, retention, destruction and use of personal data) are governed by the Data Protection Act 1998. The Act applies to all personal data - whether they are held on a computer or similar automatic system or whether they are held as part of a manual filing system.

The Data Protection Act 1998 also covers the transferring of personal data to a third party that is located in a country or territory outside the European Economic Area (EEA).

Personal data is defined as information relating to an identifiable living individual and can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

1.3 Failure to comply with the Data Protection Act 1998 could result in the prosecution not only of a Group member but also of the individual responsible for the breach in data security.

Data subjects (that is persons about whom such data is held) may also sue for compensation for damage and any associated distress suffered as a result of:

- loss or unauthorised destruction of data;
- unauthorised disclosure of, or access obtained to, data; and
- inaccurate data - i.e. data which is incorrect or misleading.

Financial penalties can be imposed on Group members by the Information Commissioner for any serious breaches of the Data Protection Act 1998. **The maximum financial penalty that the Information Commissioner can impose on a member of the Group is a fine of £500,000.**

1.4 Given the financial consequences of any serious breach of the Data Protection Act 1998, it is imperative that Group members' staff, Governing Body Members or contractors concerned with, or having access to, such data ensure that data is processed according to the principles of data protection and the rights of data subjects.

Group members' staff, Governing Body members and contractors must treat all data carefully and must not disclose any personal data to unauthorised persons (this includes parents or relatives of tenants or other data subjects).

1.5 Group members are registered individually with the Information Commission Office as a Data Controller as required by the Data Protection Act 1998. Caledonia Housing Association's Registration No is: Z5000643) whilst Cordale Housing Association's Registration No. is Z6742223

2. Policy Scope

2.1 This policy applies to:

- all Caledonia and Cordale Housing Association staff;
- all Governing Body members;
- contractors and suppliers appointed by Caledonia and/or Cordale Housing Associations; and
- any bodies or organisations working with Caledonia Housing Association and/or Cordale Housing Association in a partnership/joint-working arrangement.

3. Equal Opportunities

3.1 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.

.

4. Data Protection Principles

4.1 When processing personal information, Group members will ensure that they comply at all times with the requirements of the Data Protection legislation. This compliance will ensure all personal information that is collected is processed fairly and for lawful purposes. This information will also be stored safely and not disclosed to any other person unlawfully.

In order to achieve the requirements set out in 1.2, the Association will comply in full with the eight principles contained in Section 1 of the Data Protection Act 1998 in the following terms:

i. Data should be processed fairly and lawfully
ii. Data should be obtained for one or more specified lawful purposes
iii. Data shall be adequate, relevant and not excessive
iv. Data shall be accurate and where necessary kept up to date
v. Data is not kept longer than is necessary for its purpose
vi. Data shall be processed in accordance with subject rights under the Act
vii. Appropriate technical and organisational measures shall be taken against unauthorised/unlawful processing, loss, destruction, damage to personal data
viii. Data shall not be transferred outside the EU unless that country/territory ensures adequate level of protection for rights and freedoms of data subjects in relation to the processing of personal data

5. Responsibilities for Compliance

5.1 Each Group member, as a corporate body, is the data controller under the Act. However, the following groups/individuals also have responsibilities for data protection compliance:

- Governing Body members;
- Chief Executive and all departmental/area directors;
- all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within their respective Associations; and
- Group members' staff who process personal information as part of their duties.

The Business Services Director has overall responsibility for data protection matters within the Group, and for reporting any serious data protection breaches to the Information Commissioner.

The Business Services Director (Caledonia) and the Area Director (Cordale) are also responsible for ensuring the Data Protection Register held by the Information Commissioner Office is accurate and up to date.

6. The Rights of the Individual/Data Subject

6.1 Individuals/Data Subjects have the following rights in relation to the processing of their personal data.

- the right of access to a copy of the information comprised in their personal data;
- the right to object to processing of data that is likely to cause or is causing damage or distress;
- the right to prevent processing for the purpose of direct marketing;
- the right to object to decisions being taken by automated means;
- the right to claim compensation for damages caused by a breach of the Act; and
- the right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.

6.2 A definition of terms relating to data subjects, and examples of the types of personal data that the Group or its members may collect are listed in Appendix A of this policy.

7. Consent

7.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. With this in mind, the Group's members will always obtain consent from the individual/data subject prior to processing any personal or sensitive data.

The Group's members understand "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

7.2 Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.3 In order to apply with the requirements of the eighth data protection principle, the Group's members will obtain specific consent if an individual's data is to be transferred to a country/territory outside the European Economic Area. Furthermore, the Group's members will only transfer personal data to a country/territory that has adequate levels of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Group's members will also seek consent from an individual if their personal data is to be published on their internet site.

8. Disclosure of Data

8.1 This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent (e.g. a tenant/member of staff has consented to the Group member corresponding with a named third party);
- where the disclosure is in the legitimate interests of the Group member (e.g. disclosure to staff - personal information can be disclosed to other Group member's employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- where the Group member is legally obliged to disclose the data (e.g. Health and Safety returns, ethnic minority and disability monitoring); and
- where disclosure of data is required for the performance of a contract.

8.2 Group members have a statutory obligation to provide personal data to third party organisations such as the Police, local authorities and the Department of Work and Pensions. In cases such as this, there is no requirement for the Group member to gain consent from the data subject prior to disclosing the requested personal data. However, where there is no statutory obligation to disclose personal data to a third party, then explicit consent will be sought by the Group member from the Data Subject/individual.

8.3 The Act permits certain disclosures without consent so long as the information is requested for one or more of the purposes listed below. This type of information disclosure will only be accommodated providing the requests are supported by the appropriate legal documentation:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

9. Rights of Access to Data

9.1 In accordance with the Data Protection Act, all individuals or their authorised representatives have the right to access any personal data, which are held by Group members in electronic format and manual/paper record. This includes the right to inspect confidential personal references received by Group member about that person.

These information requests are referred in the Data Protection Act as 'Subject Access Requests' (SAR). Individuals or authorised representatives who submit SAR to a Group member will be provided all the relevant information to which they are entitled by law subject to any statutory exemptions.

9.2 Any individual who wishes to exercise this right to submit a SAR should apply in writing to the Business Services Director in respect of Caledonia Housing Association or the Area Director in respect of Cordale Housing Association. Group members reserve the right to charge a fee for SAR (currently £10). Any such request should be complied with within 40 days of receipt of the written request and, where appropriate, the £10 fee for the provision of the requested information be applied.

9.3 Where it is not possible to meet the 40 day time limit, an explanation will be provided to the individual who made the SAR.

9.4 All employee requests for access to personal data held by the Group that relates specifically to them will be directed to their line manager. The line manager will then inform the HR Manager of the request by the Group member's employee to access their personal data.

The HR Manager will make arrangements for the employee to view the file. No items or contents can be removed or copied without the permission of the HR Manager.

10. Retention & Disposal of Data

10.1 The Data Protection Act 1998 does not set out any specific minimum or maximum period for retaining personal data. Instead, the Act states personal data processed for any purpose shall not be kept longer than is necessary by the organisation.

It is therefore necessary to consider the reasons for collecting personal data and if the data should be retained when the relationship between and the individual ends, i.e. former tenants or employees.

Guidance on data retention periods is provided in the Group member's Data Protection Procedures.

10.2 The Group members will ensure at all times that personal data is disposed of in a way that protects the rights and privacy of data subjects. Typical methods employed by Group members for disposal of data including the following:

- shredding;
- disposal as confidential waste; and
- secure electronic deletion of data files.

11. Data Security

11.1 There is a duty placed on the Group members by the Data Protection Act 1998 to ensure there is appropriate security to prevent personal data held by the Group members being accidentally or deliberately compromised.

11.2 All Group members' staff, Governing Body members and appointed contractors are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to unauthorised third parties. Only authorised Group members' staff, Governing Body members and appointed contractors can access, alter, disclose or destroy personal data within the scope of their authority.

11.3 Personnel files will be stored in locked cabinets, and access to computerised records will be password protected. Staff should also ensure any personal data displayed on a PC screen cannot be viewed by an unauthorised third party either in the workplace or when using any form of digital media device in a public place.

11.4 In terms of minimising risks associated with breaches of Data Protection Act through lapses in personal IT security, staff with access to personal data should always ensure their PC is 'locked' if they need to leave their desk.

11.5 Any misuse of personal data or breaches of data security by Group members' staff, Governing Body members or contractors may result in disciplinary or legal action being taken against the individual by the Group member

11.6 Significant data breaches covered by the Data Protection Act 1998 will be reported at the earliest opportunity to the respective Governing Body, and to the Scottish Housing Regulator as a notifiable event.

12. Risk Management and Audit

12.1 The Group aims to mitigate the risk of potential financial penalties and compensation payments through failure to adhere to Data Protection legislation through the provision of training to staff on data protection issues as detailed in section 12 above. . The Group will also review this policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, an annual review of personal information held by the Association will be carried out to ensure ongoing compliance with the provisions of the data protection legislation.

12.2 Internal audit procedures will form an important part of establishing and sustaining good data protection practices. The Association will review the data it processes and collects and assess this against eight principles as listed in Section 4 of this policy. This will inform the review of our action plan to ensure compliance with the policy.

12.3 We will undertake self-assessment to periodically check our compliance with the Act; our Data Protection Policy and guidance, regulatory and good practice guidance; our registration with the Information Commissioner's Office; our working practices in the collection, processing and storage of personal information and achievement of our Action Plan.

12.4 Data protection issues will be considered as part of the Group's Risk Management Strategy, and if assessed as a priority risk area the commitment of resources will be considered to attend to the controls to mitigate these risks.

13. Training

13.1 All individuals permitted to access personal data in line with their work duties will be trained in Data Protection following the implementation of the Data Protection Policy and Guidance. All individuals with access to personal data on or behalf of the Group members must agree to undertake any relevant training that may deemed appropriate.

13.2 Data Protection training will form part of the Induction training of new employees. A copy of the Group Data Protection Policy and Guidance will be provided to all employees (including Agency Staff) and Governing Body members.

14. Policy Review

14.1 This policy will be reviewed every three years by the Group, although *ad hoc* changes will be made to the policy during the three-year period if any the following occur:

- responding to any new legislative changes in the Data Protection Act; and
- to address any weaknesses in the policy that has been identified by the Group members as a result of a breach in data security.

Appendix A

Definition of Terms

Data Subject

This refers to any living individual who is the subject of personal data. Examples of data subjects for the Group are:

- Tenants, prospective tenants and former tenants
- Governing Body members
- Employees
- Sharing owners
- Others in receipt of service
- Applicants seeking paid and non-paid employment with the a Group member

Personal Data

Personal data relates to data that can identify an individual from information which is held by Group members. It also includes any expression of opinion or view about an individual or their circumstances.

Examples of personal data include, but not limited to, the following:

- Age
- Marital status
- Housing history
- Economic status
- Allowance, benefits and grants
- Support services received
- Medical data

Sensitive Personal Data

The Act also recognises that some items of data are more sensitive than others and therefore require additional legislation to ensure appropriate handling.

Examples of sensitive personal data include, but are not limited, to the following:

- Race or ethnic origin
- Political opinions
- Religious or other beliefs
- Physical or mental health
- Criminal convictions