Group Policy:
Data Protection

Policy Owner	Lucy Docherty, Data Protection Officer
Policy Manager	Executive Director, Group Services
Approval Body	Audit & Risk Committee
Approval Date	21 July 2020

Contents

This policy is available, on request, in different languages and in other formats such as large print, audio format and braille as required.

1. Scope

1.1 This policy applies to all personal data processing carried out by River Clyde Homes ("RCH") and all personal data processing carried out by its subsidiary Home Fix Scotland Ltd ("HFS"), collectively known as the RCH Group of companies or the RCH Group.

1.2 This Group policy applies to Staff, Board and Committee members of The RCH Group.

2. Introduction

2.1 The RCH Group requires to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include tenants and their families, service users, employees (present, past and prospective), Board and Committee members, suppliers, partners and other business contacts, and members of the public. The Group must ensure that any information about individuals is collected and used lawfully, fairly and transparently, is stored securely, and is not disclosed to any third party unlawfully.

2.2 This policy is intended to provide the framework for ensuring compliance within the RCH Group with the General Data Protection Regulation (EU) 2016/679 ("the GDPR") and the Data Protection Act 2018 and any subsequent or related laws.

2.3 River Clyde Homes and Home Fix Scotland, each have legal responsibilities as Controllers when processing personal data and where acting as a processor for each other or a third party, they have responsibilities as a Processor.

2.4 This policy should be read in conjunction with the Rights of the Data Subject Procedure, the Data Breach Reporting and Response Procedure, the Information & Records Management Policy; the Information Security & Acceptable Use of ICT Policy and the Freedom of Information Policy. All RCH Group, RCH and HFS policies should be interpreted in a way that is compliant with the RCH Group Data Protection Policy.

3. Definitions

3.1 "Personal Data" (or "personal information") is defined as any information relating to an identified or identifiable natural person. 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.

3.2 A “Data Subject” is a natural individual identified or identifiable by personal data.

3.3 “Special Categories of Personal Data” is personal data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning an individual’s health, sex life or sexual orientation; or the processing of genetic or biometric data for the purpose of uniquely identifying an individual.

3.4 A “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.5 A “controller” determines the purposes and means of processing personal data.

3.6 A “processor” is responsible for processing personal data on behalf of a controller.

4. Policy Statement and Responsibilities

4.1 The RCH Group are legally obliged to comply with the data protection principles, which require that personal data shall be:

- **Principle 1** – processed lawfully, fairly and in a transparent manner in relation to individuals (“lawfulness, fairness and transparency”).
- **Principle 2** – collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”).
- **Principle 3** – adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”).
- **Principle 4** – accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”).
- **Principle 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 (“storage limitation”).
- **Principle 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 (“integrity and confidentiality” or “security”).

4.2 Additionally, the RCH Group must ensure that its companies are able to demonstrate compliance with the previous 6 principles (**Principle 7:** "Accountability").

Data Subject Rights

4.3 The individuals whose personal information we process have the following rights under Data Protection Legislation:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling (i.e. where a system takes decisions without human intervention).

4.4 The applicability of some of these rights will depend upon the lawful basis for processing. Further detail on these rights and the procedures for complying with them are set out in the Rights of the Data Subject Procedures.

Data Sharing

4.5 The RCH Group shares its data with various third parties for numerous reasons in order that its day to day activities can be carried out. To enable it to monitor compliance by these third parties with Data Protection laws, we will require the third party organisations to enter into an agreement, with the relevant RCH Group company, governing the processing of data, security measures to be implemented and responsibility for breaches.

Personal Data sharing with 'Processors'

4.6 A 'processor' is a third party that processes personal data on behalf of the data controller (RCH or HFS) and are frequently engaged if certain work is outsourced e.g. maintenance and repair works.

4.7 Data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the controller, if a data breach is suffered.

4.8 If a data processor wishes to sub-contract their processing it must obtain prior written consent from the controller to do so. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

4.9 Where a RCH Group company contracts with a third party and the contract entails the processing of personal data, it shall require the third party to enter into a contractual agreement in accordance with our model clauses.

Personal Data sharing with 'Joint Controllers'

4.10 Personal data is from time to time shared with third parties who jointly determine the processing purposes of the shared data. In such instances both the relevant RCH Group company and the third party will be processing that data in their individual capacities as data controllers and will require to enter into a Data Sharing Agreement.

Data Breaches

4.11 Personal data breaches and suspected or potential personal data breaches must be reported to the Group Data Protection Officer immediately in line with the Data Breach Reporting and Response Procedure to enable the data breach to be assessed, appropriate action to be taken and external reporting duties to the Information Commissioner's Office (ICO) to be met. Additionally, the RCH Group must assess whether the breach is likely to result in a high risk of individuals' rights and freedoms being adversely affected and if so, inform those affected without undue delay.

4.12 Personal data breaches include, but are not restricted to, the following:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Data Protection Impact Assessments

4.13 A Data Protection Impact Assessment (DPIA) is a means by which we can identify and reduce the data protection risks of a project or new processing operation.

4.14 Specified types of processing require a DPIA as well as any processing of personal data that is "likely to result in a high risk" to individuals. Certain criteria have been identified as indicators that processing is likely to be high risk. To assess whether a DPIA is mandatory the Screening Questionnaire on the RCH Group Data Protection SharePoint site should be used and if a DPIA is required the Group DPIA template, also available on the site, should be used.

4.15 The DPIA template, available on the RCH Group Data Protection SharePoint site, should be used for any major new project involving the use of personal data.

4.16 In the event that a DPIA identifies a high level of risk which cannot be reduced, the relevant RCH Group company will require to consult with the ICO before commencing the processing activity. The Group Data Protection Officer will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the Group Data Protection Officer within five working days.

4.17 **The RCH Group will ensure adherence to Principle 1 (Lawfulness, Fairness and Transparency) by**:

- ensuring that there is a lawful ground for all personal data processing prior to any new processing commencing, this includes identification of an additional condition for processing any special category or criminal conviction data and completion of an 'Appropriate Policy Document' where required by the Data Protection Act 2018 (see Appendix 1);
- being clear and open with individuals about how their information is used; and
- ensuring that all privacy notices are issued in line with Rights of the Data Subject Procedures.

4.18 The RCH Group will ensure adherence to Principle 2 (Purpose Limitation) by:

- clearly identifying and documenting our purposes for processing (Record of Processing Activities; Privacy Notices; Legitimate Interest Assessments; Appropriate Policy Documents; Data Protection Impact Assessments);
- regularly reviewing our processing and, where necessary, updating our documentation; and
- if we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

4.19 The RCH Group will ensure adherence to Principle 3 by (Data Minimisation):

- ensuring that only personal data that is required for the specified purposes is collected;
- ensuring that there is sufficient personal data to properly fulfil those purposes; and
- periodically we review that data we hold and delete anything that we don't require.

4.20 The RCH Group will ensure adherence to Principle 4 (Accuracy) by:

- ensure that any personal data created is accurate;
- ensuring that we have appropriate processes in place to check the accuracy of data we collect and, where necessary, keep it up to date; and

- where possible, providing customers and employees with direct online access to some of their personal data to enable them to check and amend their data as well as access other services.

4.21 The RCH Group will ensure adherence to Principle 5 (Storage Limitation) by:

- considering how long it requires to keep personal data for the purposes for which it is processed;
- ensuring that standard retention periods are set wherever possible to comply with documentation requirements (Data Retention Schedule);
- ensuring that personal data is reviewed in accordance with the periods set out in the Data Retention Schedule and then either erased, destroyed or anonymised where it is no longer required; and
- ensuring that there are good records management processes in place, where possible, that support the storage limitation principle, for example, by automating review periods and making effective retrieval of all relevant personal data quick and efficient.

4.22 The RCH Group will ensure adherence to Principle 6 (Integrity and Confidentiality) by:

- ensuring that appropriate technical and organisational security measures exist to ensure the confidentiality, integrity and availability of personal information; and
- ensuring that all Personal Data held by the RCH Group is stored securely and protected against unauthorised use and access.

4.23 The RCH Group will ensure adherence to Principle 7 (Accountability) by:

- through the adoption and implementation of this policy and supporting procedures;
- maintaining documentation of our processing activities, including processing purposes, data sharing and retention;
- ensuring written contracts are in place with organisations that process personal data on our behalf;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- taking a ‘data protection by design and default’ approach; and
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests.

4.24 The Chief Executive has ultimate responsibility for RCH Group compliance with data protection legislation and for enforcing compliance in relation to this policy.

4.25 The Executive Directors and the Managing Director of HFS have overall responsibility for ensuring and enforcing compliance within their respective business areas.

4.26 The Heads of Service, supported by their Senior Managers and/or Managers, have day to day operational responsibility for compliance within their business area. They should, as a minimum, ensure the following:

- all regular processing carried out within their business area, including any processing carried out on behalf of a third party, is reflected in the relevant RCH Group company Registers of Processing Activities;
- there is a lawful basis identified and documented for all personal data processing and that additional lawful conditions are identified for the processing of any special category personal data or criminal offence data;
- where consent is being relied upon, suitable records are maintained and processes are in place to act upon any withdrawal of consent;
- that Privacy Notices are being issued, or made available, to the individuals whose personal data we process;
- that personal data breaches are reported promptly to allow adherence to required timescales for any external reporting required;
- that Data Protection Impact Assessments are carried out when there is likely to be a high risk to any individuals whose data we intend to process;
- that where we provide personal data to a third party to process on our behalf, there is a written contract in place with the required terms and conditions;
- when entering into an any other arrangement with a third party that involves the regular sharing of personal data, that there is a data sharing agreement in place; and
- there are suitable processes, systems or measures in place for adhering to the Data Protection Principles and enabling customers or other data subjects to exercise their rights in relation to their personal data.

4.27 The Data Protection Officer is responsible for:

- providing advice in relation to, and monitoring compliance with, this policy and data protection, and related, legislation;
- raising awareness of data protection issues and training staff;
- maintaining the Registers of Processing Activities for RCH and HFS;
- conducting and reporting on internal audits;
- providing advice in relation to DPIAs and monitoring the DPIA process;
- reporting breaches or suspected breaches to the ICO;
- co-operating with and serving as the organisation's contact for discussions with the ICO.

4.28 All teams and employees are responsible for:

- achieving a general level of awareness of data protection and information security; and
- following procedures and practices for maintaining appropriate security of the Personal Data to which they have access.

5. Equality Impact Assessment

5.1 An EIA has been undertaken and all relevant requirements have been met. There was no negative affect on equality identified.

6. Review

6.1 This policy will be reviewed in its entirety every 3 years, unless an earlier review is required due to changes in legal, regulatory or best practice requirements, or because monitoring and reporting reveals that a change in policy is required sooner.

Appendix 1: Lawful Grounds for Processing Personal Data

1. The RCH Group are permitted to process personal data provided they are doing so on one of the following grounds:
   (a) the processing is necessary for entering into, or for the performance of, a contract, with the data subject;
   (b) the processing is necessary for the compliance with a legal obligation to which it is subject;
   (c) the processing is necessary to protect the vital interests of the data subject or another person;
   (d) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested;
   (e) the processing necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or
   (f) the processing is with the consent of the data subject.

2. The RCH Group should not rely on ground (e) legitimate interests when carrying out processing related to functions for which it is designated a public authority, further specified in the RCH Group Freedom of Information Policy.

3. Consent, as a ground for processing, will require to be used from time to time, where no other alternative ground for processing is available. In the event that RCH or HFS require to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained must be for a specific and defined purpose (i.e. general consent cannot be sought) and the appropriate records of consent must be maintained.

4. However, for special category personal data one of the following additional conditions must also be met:
   (a) Explicit consent
   (b) Employment, social security and social protection (if authorised by law)
   (c) Vital interests
   (d) Not-for-profit bodies
   (e) Made public by the data subject
   (f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

5. When relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018 and an appropriate policy document must be completed.

6. If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018 and an appropriate policy document must be completed.

7. For criminal offence data, the RCH Group must identify an additional condition in Parts 1, 2 or 3 of Schedule 1 of the DPA 2018 and an appropriate policy document must be completed.