Appendix 2

RCH Group Policy: Data Protection

Policy Owner	Group Services Director
Policy Manager	Business Planning & Compliance Manager
Approval Body	Audit & Risk Committee
Approval Date	29th April, 2024

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 the processing of personal information that is within scope of data protection legislation and carried out by River Clyde Homes ("RCH") and its subsidiary Home Fix Scotland Ltd ("HFS"), collectively known as the RCH Group.

1.2 **Processing** is defined broadly so that it covers any use of information, including holding information, and **Personal Data** is any information relating to an identified or identifiable – directly or indirectly – natural living person.

1.3 **Pseudonymised Data** is within scope of data protection legislation; only if personal data has been anonymised and the anonymisation is non-reversible is this information not regulated. [Bold terms are further outlined in the **Definitions section**.]

1.4 This Group policy applies to staff and board 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 River Clyde Homes and Home Fix Scotland, each have legal responsibilities in relation to the data processing they carry out. This policy is intended to provide the framework for ensuring the RCH Group meets its obligations under the following legislation and any subsequent or related laws:

- UK General Data Protection Regulation ("the UK GDPR")
- Data Protection Act 2018 ("DPA 2018"); and
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

2.3 This policy should be read in conjunction with the:

- Data Subject Rights Procedure;
- Data Breach Reporting and Response Procedure;
- Data Protection by Design & Default Procedures;
- Appropriate Policy Document: Our use of Special Category Data;
- Records Management Policy;

- Information Security & Acceptable Use of ICT Policy;
- ICT Security Policy; and
- Freedom of Information Policy.

2.4 Embedding Data Protection compliance will enable the RCH Group to:

- protect the rights and interests of its customers and their families, its staff and board members and any other individuals whose personal data we hold;
- protect our assets and promote business efficiency; and
- support good governance.

3. Definitions

3.1 "**Processing**" – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.2 "**Personal Data/ Information**" – any information relating to an identified or identifiable – directly or indirectly – natural living person.

Identifiable can be with reference to an identifier such as:

- a name or an identification number;
- location data;
- an online identifier; or

it can be with reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person. This includes where a person can be identified by combining the information being processed with other information from another accessible source.

3.3 A "**Data Subject**" is the identified or identifiable living individual to whom personal data relates.

3.4 "**Pseudonymised Data**" – data that can no longer be attributed to a specific data subject without the use of additional information that is kept separately and subject to appropriate measures to prevent attribution to an identified or identifiable person. Pseudonymisation involves the replacement of identifiers with a reference that does not enable identification.

3.5 "**Special Categories of Personal Data**" are afforded additional protection because their use could create significant risks to the individual's fundamental rights and freedoms. These are:

- 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 data** or **biometric data** for the purpose of uniquely identifying an individual.

3.6 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.

3.7 A "**controller**" determines the purposes and means of processing personal data.

3.8 **"Joint Controllers"**: parties who decide the purposes and means of processing together – they have the same or shared purposes. Controllers will not be joint controllers if they are processing the same data for different purposes.

3.9 A "**processor**" is responsible for processing personal data on behalf of a controller and must process data in line with the relevant controller's instructions.

3.10 "**RCH Group Personal Data**" – personal data that either RCH or HFS is the controller of. For example, staff data or customer data.

4. Policy Statement

4.1 The RCH Group are committed to transparent, lawful, fair and proportionate processing of personal data. This includes all personal data we process about customers, staff or those who interact with us. Our processing must comply with the Data Protection Principles outlined in Appendix 1.

Data Subject Rights

4.2 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).

4.3 The applicability of some of these rights will depend upon the lawful basis for processing, which is required to be identified under the Lawfulness, Fairness & Transparency Principle. The RCH Group will adhere to the Rights of the Data Subject Procedures when receiving a request from an individual to exercise a right in relation to their data.

Data Sharing

4.4 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.

Personal Data sharing with 'Processors'

4.5 When we enter into a contract with another party to carry out a piece of work, service or similar and that contract requires that personal information is shared with the third party or that the third party will collect or create personal information on our behalf, then we must:

- Ensure that there is a legally binding contract that covers all the terms defined in Article 28 of the UK GDPR and also specifies the personal data processing related to the contract (subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects).
- The data sharing related to the contract must comply with the data protection principles.
- Choose an appropriate Processor (Contractor) that provides sufficient guarantees that they will implement appropriate technical and organisational measures. To support the assessment of a processor's competence to process RCH Group Personal Data an exercise will be carried out when procuring services or works that involve RCH Group Personal Data.
- Ensure that transfers of data outside of the UK are avoided where possible. If it is necessary to carry out a restricted transfer, then the transfer must be covered by:
    - adequacy regulations or decisions;
    - appropriate safeguards as set out in Article 46 of the UK GDPR (this will require a transfer risk assessment to be carried out); or
    - an exception as set out in Article 49 of the UK GDPR.

Personal Data sharing with 'Controllers'

4.6 It may be necessary or desirable for an RCH Group company to share personal information with other Controllers at times. This can be as separate or independent controllers or as Joint Controllers. Consideration of specific

arrangements are a legal requirement in relation to Joint Controllers and this can be documented as part of a Data Sharing Agreement.

4.7 The RCH Group Data Sharing Guidance (Appendix 2) should be referred to prior to making a decision to share data and entering into a Data Sharing Agreement.

Personal Data Breaches

4.8 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.

4.9 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

4.10 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. A DPIA must be carried out where processing of personal data that is "likely to result in a high risk" to individuals.

4.11 The Data Protection by Design and Default Procedures set out the procedure for assessing processing of personal data perceived to be of high risk as well as the process for completing a DPIA.

4.12 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.

Privacy Notices

4.13 We publish public facing privacy notices on our website and staff privacy notices on our intranet and keep these up to date. We also provide additional relevant timely privacy information when we are collecting additional information from individuals.

4.14 These document the details of the relevant personal data processing including the lawful bases of processing as well as the lawful conditions for special categories of personal data or criminal offence data. Further information on the management of Privacy Notices is detailed in Rights of the Data Subject Procedures under the right to be informed.

Training

4.15 We require all staff to undertake mandatory training on information compliance and security at their induction and then on annual basis thereafter.

5. Roles & Responsibilities

5.1 The RCH Group Audit and Risk Committee is responsible for the overview and scrutiny of information governance arrangements and associated risks as it has delegated responsibility for overseeing the overall risk environment for the RCH Group.

5.2 The Chief Executive and the rest of the Executive Leadership Team are responsible for RCH Group compliance with data protection legislation and for enforcing compliance in relation to this policy and related procedures.

5.3 The RCH Group Data Protection Officer (Business Planning & Compliance Manager) is primarily responsible for advising on and assessing our compliance with UK data protection legislation and making recommendations to improve compliance. The Group Data Protection Officer will report as necessary to the Group Audit & Risk Committee.

5.4 Senior Management and Management, 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.

5.5 The Information Compliance Team will provide advice, support and guidance on information governance and data protection compliance.

5.6 All teams and employees have responsibility for:

- achieving a general level of awareness of data protection and information security;
- familiarising themselves with and adhering to existing procedures, practices and guidance; and
- maintaining appropriate security of the Personal Data to which they have access.

6. Monitoring of this policy

6.1 Compliance with this policy will be monitored by the Data Protection Officer and reported to the Group Audit & Risk Committee.

7. Equality, Diversity and Inclusion

7.1 The RCH Group will apply this policy fairly and consistently. In implementing this policy, we will not directly or indirectly discriminate against any person or group of people because of their race, religion or belief, gender, disability, age, sexual orientation, or any other grounds. Our commitment to equality and fairness will apply irrespective of factors such as age, disability, gender reassignment, marital or civil partnership status, pregnancy or maternity, race, religion or belief, sex, sexual orientation, or other personal attributes.

8. Review

8.1 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: Data Protection Principles

The data protection principles require that personal data shall be:

- **Principle 1** – processed lawfully, fairly and in a transparent manner in relation to individuals ("**lawfulness, fairness and transparency**").
    - **All personal data** requires a Lawful Basis identified in advance of processing:
        - **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
        - **Contract:** the processing is necessary for a contract an RCH Group company has **with the individual**, or because they have asked us to take specific steps before entering into a contract.
        - **Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).
        - **Vital interests**: the processing is necessary to protect someone's life.
        - **Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. (This applies to our public tasks as a Registered Social Landlord.)
        - **Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot be used for processing data to perform our public tasks as a Registered Social Landlord.)
    - **Special Category Data** requires an additional Article 9 Lawful Condition for processing & where one of the following conditions is relied upon, a relevant condition under Part 1 or 2 of Schedule 1 of the Data Protection Act 2018 must be identified and the Appropriate Policy Document updated:
        - employment, social security and social protection
        - substantial public interest
        - health and social care

        - public health
        - archiving, research and statistics
    - **Criminal Offence Data** must also meet requirements of Article 10 and a condition under Schedule 1 of the DPA 2018 and the Appropriate Policy Document must be updated.
    - Processing must be **otherwise lawful.**
    - **Privacy Notices** must be issued at the point of data collection, or within 1 month if data received from a third party e.g., Factoring Customers. As additional information is collected just-in-time privacy information should be provided. (See Rights of the Data Subject Procedures)
    - We must be **clear and open** with individuals about their information is used. (See Rights of the Data Subject Procedures)

- **Principle 2** – collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("**purpose limitation**").
    - Purposes for processing will be clearly identified and documented (Record of Processing Activities; Privacy Notices; Legitimate Interest Assessments. Appropriate Policy Documents; Data Protection Impact Assessments).
    - Processing will be regularly reviewed and, where necessary, documentation updated and communicated.
    - 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.

- **Principle 3** – adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**").
    - Only collect personal data that is required for the specified purposes.
    - Ensure that there is sufficient personal data to properly fulfil those purposes.
    - Periodically review data we hold and delete anything not required.

- **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**").
    - Personal data must be accurate and we must have appropriate processes in place to check the accuracy of data we collect, and, where necessary, to keep it up to date.
    - Where possible, we provide 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.

- **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**").

- We consider how long we require to keep personal data in relation to the purposes for which it was collected.
- We ensure that retention periods are set wherever possible and detailed in Privacy Notices or Privacy Information; our Records Retention Schedule and relevant policy, procedure or process documentation;
- Personal data is reviewed in accordance with the periods set and then either erased, destroyed or anonymised where it is no longer required.
- We ensure 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.

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

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

- through the 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;
- documenting appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- taking a 'data protection by design and default' approach.
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

Appendix 2: Data Sharing Guidance

Scope of this Guidance:

This guidance covers data sharing with other controllers. It does not cover data shared with processors, for example contractors who require to process our personal data for the purposes of fulfilling a contract with us, e.g., providing a service. It does not cover sharing data within the RCH Group.

Data sharing examples:

- a one-way or reciprocal exchange of information
- several organisations pooling information and making it available to each other or a third party or parties
- an organisation providing another organisation with access to personal data on its IT systems
- data sharing on a routine, systematic basis for an established purpose
- one-off exceptional or ad hoc data sharing
- one off data sharing in an urgent or emergency situation

DATA SHARING CHECKLIST

Check whether the sharing is justified

Key points to consider:

- ☐ What is the sharing meant to achieve?
- ☐ Have the potential benefits and risks to individuals of sharing or not sharing been assessed?
- ☐ Is the sharing proportionate to the issue you are addressing?
- ☐ Could the objective be achieved without sharing personal data, or by sharing less personal data?
- ☐ What safeguards can you put in place to minimise the risks or potential adverse effects of sharing?
- ☐ Is there an applicable exemption in the Data Protection Act 2018 (DPA 2018)?

Consider doing a Data Protection Impact Assessment

Decide whether you need to carry out a DPIA:

- ☐ You must do a DPIA for data sharing that is likely to result in a high risk to individuals. This will depend on the nature, scope, context and purposes of the sharing. Refer to RCH Group screening questions.
- ☐ For any data sharing plans, you may find it useful to follow the DPIA process as a flexible and scalable tool to suit your project.

If you decide to share

It is good practice to have a data sharing agreement. As well as considering the key points above, your data sharing agreement should cover the following issues. You should ensure you cover these matters in any event, whether or not you have a formal agreement in place:

- ☐ What information will you share?
- ☐ Is any of it special category data? What additional safeguards will you have in place?
- ☐ How should you share the information?
  - You must share the information securely.
  - You must ensure you are giving the information to the right recipient.
- ☐ What is to happen to the data at every stage?
- ☐ What organisation(s) will be involved? You all need to be clear about your respective roles.
- ☐ Who in each organisation can access the shared data? Ensure it is restricted to authorised personnel in each organisation.
- ☐ How will you comply with your transparency obligations?
  - Consider what you need to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.
  - Consider whether you have obtained the personal data from a source other than the individual.
  - Decide what arrangements need to be in place to comply with individuals' information rights.
- ☐ What quality checks are appropriate to ensure the shared data is accurate and up to date?
- ☐ What technical and organisational measures are appropriate to ensure the security of the data?
- ☐ What common retention periods for data do you all agree to?
- ☐ What processes do you need to ensure secure deletion takes place?
- ☐ When should regular reviews of the data sharing arrangement take place?

If a data sharing agreement is required, liaise with the Data Protection Officer providing the information described above. Data sharing agreements should be signed by a Senior Manager or Head of Service and reviewed regularly to ensure the information is up to date and accurate and to examine how the agreement is working.

Once a data sharing agreement has been signed by both parties, provide a copy of the signed agreement to DataProtection@riverclydehomes.org.uk.

Decide what your lawful basis is for sharing the data

Key points to consider:

- ☐ What is the nature of the data and the purpose for sharing it, as well as the scope and context?
- ☐ Are you relying of legitimate interests as a lawful basis? If so, you should carry out a legitimate interests assessment (LIA) to ensure we can justify using this basis.
- ☐ Is any of the data either special category data or criminal offence data? If so, you need to identify additional conditions.

Check whether you have the power to share

Key points to consider:

- ☐ Our statutory housing functions
- ☐ The nature of the information you have been asked to share.
- ☐ Whether there are any legal requirements that need to be met when sharing the data – such as copyright or a duty of confidence, or any prohibitions.
- ☐ Whether there is a legal obligation or other legal requirement about sharing information – such as a statutory requirement, a court order or common law.

Document your decision

Document your data sharing decision and your reasoning – whether or not you share the information. You can record your decision using the Data Sharing Decision Form.

If you shared information you should document:

- ☐ the justification for sharing;
- ☐ what information was shared and for what purpose;
- ☐ who it was shared with;
- ☐ when and how it was shared;

- ☐ whether the information was shared with or without consent, and how that was recorded;
- ☐ the lawful basis for processing and any additional conditions applicable;
- ☐ individuals' rights;
- ☐ data protection impact assessment reports;
- ☐ compliance with any DPO advice given (where applicable);
- ☐ evidence of the steps you have taken to comply with the GDPR and the DPA 2018 as appropriate; and
- ☐ where you have reviewed and updated your accountability measures at appropriate intervals.