Privacy Policy

Reference / Issue No:	G13	1
Date of this version:	May 2018	
Next review due:	May 2021	
Lead responsibility:	Governance	
Contents:	90 pages	5 appendices

Contents

1. Introduction

1.1 Fife Housing Group is a trading name of Fife Housing Association Ltd and PACT Enterprises Ltd.

Fife Housing Group (hereinafter 'the Group') is committed to ensuring the secure and safe management of data held by the Group in relation to customers, colleagues and other individuals. The Group's colleagues have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Group needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Group has a relationship with. The Group manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the General Data Protection Regulations (GDPR).

This Policy sets out the Group's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

Appendix 1 hereto details the Group's related policies.

2. Legislation

2.1 It is a legal requirement that the Group process data correctly; the Group must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) The General Data Protection Regulation (EU) 2016/679 ('the GDPR');
(b) The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(c) Any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3. Data

3.1 The Group holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the Group is detailed within

the Fair Processing Notice at Appendix 2 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.2 'Personal Data' is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Group.

3.3 The Group also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is 'Special Category Personal Data' or 'Sensitive Personal Data'.

4. Processing of Personal Data

4.1 The Group is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Group and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Group's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Group's official authority; or
- Processing is necessary for the purposes of legitimate interests.

5. Fair Processing Notice

5.1 The Group has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by the Group. This FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

5.2 The Fair Processing Notice (FPN) at Appendix 2 sets out the Personal Data processed by the Group and the basis for that Processing. This document is provided to all of the Group's customers at the outset of processing their data

6. Employees

6.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Group. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to employees at the same time as their Contract of Employment.

6.2 A copy of any employee's Personal Data held by the Group is available upon written request by that employee from the Group's Director of Human Resources and Business Support.

7. Consent

7.1 Consent as a ground of processing will require to be used from time to time by the Group when processing Personal Data. It should be used by the Group where no other alternative ground for processing is available. In the event that the Group requires 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 by the Group must be for a specific and defined purpose (i.e. general consent cannot be sought).

8. Processing of Special Category Personal Data or Sensitive Personal Data

8.1 In the event that the Group processes Special Category Personal Data or Sensitive Personal Data, the Group must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

9. Data Sharing

9.1 The Group shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Group's relevant policies and procedures. In order that the Group can monitor compliance by these third parties with Data Protection laws, the Group will require the third party organisations to enter in to an Agreement with the Group governing the processing of data, security measures to be implemented and responsibility for breaches.

10. Data Sharing

10.1 Personal data is from time to time shared amongst the Group and third parties who require to process personal data that the Group process as well. Both the Group and the third party will be processing that data in their individual capacities as data controllers.

10.2 Where the Group shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Group in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

11. Data Processors

11.1 A data processor is a third party entity that processes personal data on behalf of the Group, and are frequently engaged if certain of the Group's work is outsourced (e.g. payroll, maintenance and repair works).

1.2 A data processor must comply with Data Protection laws. The Group's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Group if a data breach is suffered.

1.3 If a data processor wishes to sub-contract their processing, prior written consent of the Group must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

1.4 Where the Group contracts with a third party to process personal data held by the Group, it shall require the third party to enter in to a Data Protection Addendum with the Group in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

12. Data Storage and Security

12.1 All Personal Data held by the Group must be stored securely, whether electronically or in paper format.

13. Paper Storage

13.1 If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Group's storage provisions.

14. Electronic Storage

14.1 Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Group's data processors or those with whom the Group has entered in to a Data Sharing Agreement. If Personal

data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

15. Breaches

15.1 A data breach can occur at any point when handling Personal Data and the Group has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

16. Internal Reporting

16.1 The Group takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data Protection Officer (DPO) must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Group must seek to contain the breach by whatever means available;
- The DPO must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and data subjects affected and do so in accordance with this clause 7; and
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

17. Reporting to the Information Commissioner's Office (ICO)

17.1 The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

18. Data Protection Officer (DPO)

18.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Group with Data Protection laws. The Group has elected to appoint a Data Protection Officer whose details are noted on the Group's website and contained within the Fair Processing Notice at Appendix 3 hereto.

18.2 The DPO will be responsible for:

18.2.1 Monitoring the Group's compliance with Data Protection laws and this Policy.

18.2.2 Co-operating with and serving as the Group's contact for discussions with the ICO.

18.2.3 Reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

19. Data Subject Rights

19.1 Certain rights are provided to data subjects under the GDPR. Data subjects are entitled to view the personal data held about them by the Group, whether in written or electronic form.

19.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Group's processing of their data. These rights are notified to the Group's tenants and other customers in the Group's Fair Processing Notice.

20. Subject Access Requests

20.1 Data subjects are permitted to view their data held by the Group upon making a request to do so (a Subject Access Request). The Group must respond to the Subject Access Request within one month of the date of receipt of the request. The Group:

20.1.1 Must provide the data subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.

20.1.2 Where the Personal Data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that Personal Data to the data subject who has made the Subject Access Request.

20.1.3 Where the Group does not hold the Personal Data sought by the data subject, it must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

21. The Right to be Forgotten

21.1 A data subject can exercise their right to be forgotten by submitting a request in writing to the Group seeking that the Group erase the data subject's Personal Data in its entirety.

21.2 Each request received by the Group will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

22. The Right to Restrict or Object to Processing

22.1 A data subject may request that the Group restrict its processing of the data subject's Personal Data, or object to the processing of that data.

22.2 In the event that any direct marketing is undertaken from time to time by the Group, a data subject has an absolute right to object to processing of this nature by the Group, and if the Group receives a written request to cease processing for this purpose, then it must do so immediately.

22.3 Each request received by the Group will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

23. Privacy Impact Assessments ('PIAs')

23.1 These are a means of assisting the Group in identifying and reducing the risks that our operations have on personal privacy of data subjects.

23.2 The Group shall:

23.2.1 Carry out a PIA before undertaking a project or processing activity which poses a 'high risk' to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data.

23.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

23.3 The Group will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer (DPO) will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

24. Archiving, Retention and Destruction of Data

24.1 The Group cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Group shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within the table at Appendix 5 hereto.

List of Appendices

1. Openness and Confidentiality Policy
2. Fair Processing Notice
3. Data Sharing Agreement
4. Data Processor Addendum
5. Data Retention Policy

Appendix 1

Openness and Confidentiality Policy

Reference/Issue No:	G/10	5
Date of this version:	May 2018	
Next review due:	November 2020	
Lead responsibility:	Governance	
Contents:	10 pages	0 appendices

1. Introduction

1.1 Fife Housing Group (FHG) ('the Group') is the trading name for the group structure comprising Fife Housing Association and PACT Enterprises.

1.2 We hold personal data about our employees, tenants, partners, suppliers and other individuals for a variety of business purposes.

1.3 This policy sets out how we seek to protect personal data and ensure that colleagues, Board members and contractors understand the rules governing their use of personal data to which they have access in the course of their work.

1.4 This policy also informs tenants and other customers how their data will be used and protected in accordance with legislation.

1.5 In particular, this policy requires colleagues to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.6 We have registered with the Information Commissioner as a Data Controller under the Data Protection Act and ensure that our practices in the handling of personal information are of a high standard and comply fully with the Act.

2. Scope

2.1 This policy applies to all employees (whether permanent, temporary or agency), Board members, appointed agents, partners, consultants and contractors.

2.2 Compliance with this policy is a condition of employment with FHG and any breach of this policy may result in disciplinary action, which could include dismissal and possible legal action.

2.3 All data/information processed by FHG is covered by this policy.

3. Definitions

Element	Detail
Business purposes	The purposes for which personal data may be used by FHG. Operational: housing applications, lettings, references, welfare benefits, third party referrals, correspondence, debt management and safeguarding. Employment: personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: ✓ Processing applications for housing and related services;

Element	Detail
	✓ Collection of rent and other payments that are due; ✓ Compliance with our legal, regulatory and corporate governance obligations and good practice; ✓ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests; ✓ Ensuring business policies are adhered to (such as policies covering email and internet use); ✓ Operational reasons, such as recording transactions, training and quality control; ✓ Ensuring the confidentiality of commercially sensitive information; ✓ Security vetting (Protecting Vulnerable Groups (PVG), Standard and Basic Disclosure); ✓ Safeguarding; ✓ Credit scoring and checking; ✓ Investigating complaints; ✓ Checking references; ✓ Ensuring safe working practices; ✓ Monitoring and managing colleagues' access to systems and facilities; ✓ Colleagues' absences, administration and assessments; ✓ Monitoring colleagues' conduct and disciplinary matters; ✓ Marketing our business; and ✓ Improving services.
Personal data	Information relating to identifiable individuals, such as in operational terms - housing applicants, income, welfare benefits, payment details, suppliers, consultants, contractors and marketing contacts. In employment terms - job applicants, current and former employees, agency, contract and any other colleagues. Personal data we gather may include: operationally - household composition, contact details, age, income, welfare benefits, nationality. In employment terms this may include - individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal	Personal data about an individual's racial or ethnic origin, sexual orientation, political opinions, religious or similar beliefs, trade union

Element	Detail
data	membership (or non-membership), physical or mental health or condition, criminal offences, safeguarding or related proceedings - any use of sensitive personal data should be strictly controlled in accordance with this policy.
Data Processing Principles	There are six data Processing Principles: **Principle 1: Fair and lawful:** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met (see Appendix 1), and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (see Appendix 2) is also met. **Principle 2: Purpose:** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. **Principle 3: Adequacy:** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. **Principle 4: Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. **Principle 5: Retention:** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. **Principle 6: Rights:** Personal data shall be processed in accordance with the rights of data subjects under this Act. Furthermore, appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Additionally personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Processing	Of data or information including obtaining, recording, holding, organising, adapting, consulting, retrieving or otherwise performing some operation on it. Processing also includes disclosure of data and

Element	Detail
	destroying data or information.
Data Subject	Data Subject means an individual who is the subject of personal data.
Data Controller	Is a person or organisation who decides how personal data is to be processed and for what purpose. Fife Housing Association is the data controller not individual colleagues.

4. Data processing requirements

4.1 Consent

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

4.2 The processing of all data must be:

- Necessary to deliver our services;
- In our legitimate interests and not unduly prejudicial to the individual's privacy; and
- In most cases, applicable to routine business data processing activities.

4.3 **Privacy Notice –** our website contains a Privacy Notice to clients on data protection. The notice:

- Sets out the purposes for which we hold personal data on customers and employees;
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers; and
- Provides that customers have a right of access to the personal data that we hold about them.

4.4 Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

4.5 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We

will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

4.6 **Your personal data**

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DPO so that they can update your records.

4.7 **Data security**

FHG must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

4.8 **Storing data securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it;
- Printed data should be shredded or securely disposed of when it is no longer needed;
- Data stored on a computer should be protected by strong passwords that are changed regularly;
- Personal data must not be stored on portable media;
- The DPO must approve any Cloud service used to store data;
- Servers containing personal data must be kept in a secure location, away from general office space;
- Data should be regularly backed-up in line with FHG's back-up procedures;
- Personal data should never be saved directly to the desktop or screen of mobile devices such as laptops, tablets, SurfacePro or smartphones; and
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

4.9 **Data retention**

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

5. Individual's rights

5.1 Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This is known as a Subject Access Request (SAR) and these requests should be referred immediately to the DPO for response. If you are the person submitting the Request we may need to ask you for further information to help us to comply.

Please contact the DPO if you would like to verify, correct or request information that we hold about you. There are some restrictions on the information to which you are entitled under data protection legislation however where we are permitted to provide you with the information we will.

The current rights of access are summarised below:

- To be told what personal data is being processed, and if so why and to whom that data may be disclosed;
- Be given a copy of the information or data in an intelligible form. (The data subject is not entitled to a copy of the information held on him/her in a permanent form if the supply of such a copy is not possible or would involve 'disproportionate effort';
- Be told the sources of the data;
- To prevent processing likely to cause damage or distress;
- To prevent direct marketing;
- To require a data controller not to make a decision based solely on automated means, which sufficiently affect him or her;
- To receive compensation from the data controller for a proven breach of the Data Protection Act;
- To have any inaccurate personal data erased and destroyed; and

Note that requests for information from the data subject must be in writing.

5.2 Tenants, employees and other individuals about whom FHG holds personal information, will have the right to access the information, unless it is exempt under the Data Protection Act.

5.3 We aim to respond to SARs within 20 working days.

5.4 In processing data in accordance with the individual's rights:

- FHG will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO and Communications and Marketing Manager about any such request.

- FHG will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.
- Colleagues must contact the Communications and Marketing Manager for advice on direct marketing before starting any new direct marketing activity.

5.5 Data which has been provided to FHG, in confidence, by a third party such as employment references or tenancy reports cannot be disclosed to the data subject. The data subject should make direct contact with the third party in the event that they wish to access this information. Requests for data from third parties should specifically ask if the data provided can be shared with the data subject.

6. Training

All colleagues will receive training on this policy. New colleagues will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure. Completion of training is compulsory for all colleagues.

Training will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Members of the FHG and PACT Boards will be encouraged to attend future awareness training arranged for employees.

Appointed agents and contractors – any contractor or agent employed directly or indirectly by FHG should sign a confidentiality agreement before being granted access to data.

7. General Data Protection Regulation (GDPR) provisions

GDPR will become the new legal framework in the EU effective from 25 May 2018. The UK Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

With many UK businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. The aim of the GDPR is to align data protection policies across the EU members.

Where not specified previously in this policy, the following provisions will be in effect within FHG by 25 May 2018.

7.1 **Privacy Notice - transparency of data protection**

Being transparent and providing accessible information to individuals about how we will use their personal data is important for FHG. Further information on how we collect data and what we will do with it, can be found in our Fair Processing Notice (FPN).

7.2 **Conditions for processing**

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All colleagues who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

7.3 **Justification for personal data**

We will process personal data in compliance with all six data protection principles outlined in Appendix 1. We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

7.4 **Consent**

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

7.5 **Criminal record checks**

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

7.6 **Data portability**

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

7.7 **Right to be forgotten**

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

7.8 **Privacy by design and default**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all ICT projects commence with a Privacy Plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

7.9 **International data transfers**

We may transfer, store or process your information outside the UK and or European Economic Area (EEA). By submitting your personal information to us you agree to this transfer, storage or processing.

Where information is transferred, stored or processed outside the UK or EEA we take all reasonable steps to ensure that there are adequate safeguards in place to protect your information.

7.10 **Data audit and Register**

Regular data audits to manage and mitigate risks will inform the Data Register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

8. Roles and responsibilities

8.1 The Board is ultimately responsible for ensuring openness and accountability is established within FHG and they will achieve this through establishment of key policies and delegation.

8.2 FHG's Director of Finance and Governance, who is also the Company Secretary, is responsible for ensuring that this policy is consulted on with Board and Committee members and for its review, implementation and proper application, in accordance with the agreed timetable.

8.3 As our Data Protection Officer, the Director of Finance and Governance has overall responsibility for the effective implementation of this policy.

8.4 The Data Protection Officer's responsibilities include:

- Keeping the Board and Committees updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Arranging data protection training and advice for all colleagues, members and those included in this policy;
- Answering questions on data protection from colleagues, Board members and other stakeholders;
- Responding to individuals such as tenants, applicants and employees who wish to know which data is being held on them by either Fife Housing Association or PACT Enterprises; and

- Checking and approving with third parties that handle the company's data any contracts or agreements regarding data processing.

8.5 Responsibilities of the ICT Project Manager regarding openness and confidentiality:

- Ensure all systems, services, software, contractors, suppliers and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly; and
- Ensuring that all third-party services, for example software providers, Cloud services, that the company is using or considering using to store or process data are operating with data protection requirements equivalent to or greater than those at FHG.

8.6 Responsibilities of the Communications and Marketing Manager regarding openness and confidentiality:

- Approving privacy and data protection statements attached to emails, website and other marketing copy;
- Addressing data protection queries from tenants, target audiences or media outlets; and
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection legislation and this policy.

8.7 Responsibilities of the Director of Human Resources and Business Support regarding openness and confidentiality:

- New employees – this policy will be made available to all new employees as part of their induction; and
- Existing employees – awareness sessions will be arranged periodically; and
- Addressing data protection queries from employees.

8.8 The Business Leadership Team (BLT) will ensure that personal data processed by their team is included in FHG's Data Protection Register entry, is kept up-to-date and complies with this policy's principles. It is the responsibility of each member of BLT to ensure that this policy and associated procedures are applied within their own team.

8.9 Each team will review the method of collecting data and will obtain the express consent of the data subject to process this data. A standard paragraph will be included to all forms etc. with a tick box requesting that the data subject gives express consent to the processing of their data.

8.10 All colleagues have a responsibility to fully comply with the requirements of the Data Protection Act, the GDPR and this policy. When involved in requesting information, colleagues will explain why the information is necessary, what it is to be used for, and who will have access to it.

9. Performance management

9.1 All colleagues and partners have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary;
- Maintain a register of compliance failures; and
- Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures.

9.2 Any concerns regarding the adherence to this policy will be reported to the Board at the earliest opportunity.

10. Review

10.1 This policy is due to be reviewed every three years - or earlier if a material change requires this.

Appendix 1

Schedule 2 [Data Protection Act 1998]

Processing data is lawful when one of the following conditions is met:

1. The data subject has given active 'specific and informed' consent to the way in which it is proposed their personal data is to be processed. Silence cannot be taken as consent.
2. The processing is necessary for the purpose of a contract involving the data subject.
3. The processing is necessary to comply with the data controller's legal obligations.
4. The processing is necessary to protect the vital interests of the data subject. Guidance issued by the Data Protection Registrar is that this condition may only be employed in life and death situations.
5. The processing is necessary for the administration of justice: for the exercise of statutory functions; for the exercise of the functions of government or other functions of a public nature exercised in the public interest (for example, those of a local authority).
6. The processing is necessary for the purposes of the legitimate interests of the data controller or third parties to whom data is disclosed. This condition will not be available where the rights and freedoms or legitimate interests of the data subject make such processing unwarranted. The Secretary of State makes Regulations clarifying when this condition may be used.

Appendix 2

Schedule 3 [Data Protection Act 1998]

1. The data subject has given their explicit consent to the particular processing of sensitive personal data. A 'blanket consent' will not suffice. The most obvious way of doing this would be by obtaining the person's signature on a form with the relevant details printed there.
2. The processing is necessary in connection with employment rights and obligations.
3. The processing is necessary to protect the vital interests ('life or death') of the data subject where s/he cannot give consent or the consent cannot be reasonably obtained.
4. The processing is necessary to protect the vital interests of another person and the data subject unreasonably refuses the consent.
5. The processing is carried out by certain voluntary organisations on its members' data.
6. The data subject has already deliberately made the information public.
7. The processing is necessary for the purpose of legal proceedings, taking legal advice, or establishing, exercising or defending legal rights or for the administration of justice. Accordingly, disclosure of sensitive personal data in the context of an anti-social behaviour court case is permitted, as long as it is necessary.
8. The processing is necessary for the exercise of statutory functions or governmental functions.
9. The processing is necessary for medical purposes.
10. The processing relates to racial or ethnic data, is necessary for equal opportunities purposes, and there are safeguards for the rights or freedom of the data subject.

Appendix 2

Fife Housing Group
General Data Protection Regulation (GDPR) Fair Processing Notice

(How we use your personal information)

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Fife Housing Group is a trading name of Fife Housing Association Ltd and PACT Enterprises Ltd.

Fife Housing Association Ltd, a Scottish Charity (Scottish Charity Number SC025647), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2476 R(S) and / or PACT Enterprises Ltd, Company Registration No.SC375254, both having their Registered Office at 7 Pitreavie Court, Pitreavie Business Park, Dunfermline, Fife, KY11 8UU ('**we**' or '**us**'), take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 1998 and the General Data Protection Regulation (EU) 2016/679 which is applicable from 25 May 2018, together with any domestic laws subsequently enacted.

Fife Housing Group are notified as a Data Controller with the Office of the Information Commissioner under registration number Z4669248, while Pact Enterprises Ltd are notified under registration number Z3197255, and we are the data controllers of any personal data that you provide to us.

Our Data Protection Officer is Derek Banks. Any questions relating to this notice and our privacy practices should be sent to derek.banks@fifehg.org.uk.

How we collect information from you and what information we collect

We collect information about you and other members of your household:

- When you apply for housing with us, become a tenant or board member, request services/repairs, enter in to a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details;
- When you apply to become a shareholding member;
- From your use of our online services, whether to report any tenancy/factor-related issues, make a complaint or otherwise;
- If you have any involvement in anti-social behaviour issues;
- From your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information);

- When you engage with us on social media, attend any of our events and enter prize draws or competitions; and
- When you visit our office, where our CCTV systems may record your image; and
- When you have given a third party permission to share the information they hold about you with us.

We may collect or currently hold the following information about you and other members of your household:

- Name
- Address;
- Telephone number(s);
- E-mail address;
- Date of birth;
- National Insurance Number;
- Ethnic origin, gender identity, sexual orientation and religion;
- Next of kin (name and contact details);
- Current employment details;
- Copies of documents you provide to prove your income. These may include details of your full name, address, national insurance number, income and employer;
- Copies of documents you provide to prove your age or identity. These will include details of your full name, address, date of birth and facial image. If you provide a passport, the data will also include your place of birth, gender and nationality.
- Medical details, disabilities, vulnerabilities and support needs;
- Criminal background information;
- Payments made by you to us;
- Details of your interactions with us including calls you make to us (which may be monitored and recorded);
- Your social media username, if you interact with us through those channels; and
- Your image may also be recorded on CCTV when you visit our office.

We may receive the following information about you and the members of your household from third parties:

- Personal information, including your name, address, telephone number, e-mail address, date of birth, national insurance number, gender, ethnic origin, level and type of income, medical details/support needs, your current housing situation, immigration status and criminal background information from Fife Housing Register;
- Benefits information, including awards of Housing Benefit/Universal Credit;
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour; and

- Referrals from Local Authority departments and relevant details from other support services, Government and credit reference agencies.

Why we need this information about you and how it will be used

We need your information and will use your information:

- To undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;
- To enable us to supply you with the services and information which you have requested;
- To enable us to respond to your repair request, housing application and complaints made;
- To analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- To contact you in order to send you details of any changes to our suppliers which may affect you;
- To contact you for your views on our products and services;
- To provide you with information relevant to your tenancy or other association with us;
- To protect our customers, premises and assets from crime, we operate a CCTV system at our office which records images for security. We do this on the basis of our legitimate business interests. If we discover any criminal activity or alleged criminal activity through our use of CCTV, fraud monitoring and suspicious transaction monitoring, we will process this data for the purposes of preventing or detecting unlawful acts;
- To administer any of our prize draws or competitions which you enter, based on your consent given at the time of entering;
- To ensure the safety of our colleagues and contractors; and
- For all other purposes consistent with the proper performance of our operations and business.

Sharing of your information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK. We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merged with another business entity, your information may be disclosed to our new business partners or owners;
- If we require further confirmation of your ability to meet your financial commitments your information may be disclosed to credit reference agencies, failure to meet these financial commitments may also result in your information being shared with third parties to assist with the recovery of monies due;
- If we instruct repair or maintenance works, your information may be disclosed to any contractor;

- If we are investigating a complaint or criminal activity, information may be disclosed to Police Scotland, Local Authority departments, Government and other agencies, Scottish Fire and Rescue Service, solicitors and others involved in any complaint, whether investigating the complaint or otherwise;
- If we believe it to be necessary, we may record our interactions with you and share these recordings with our lone worker protection service;
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies, the Local Authority and other Government agencies);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department of Work and Pensions;
- If we have reason to instigate legal action your information may be disclosed to third parties including Sheriff Officers and solicitors;
- If we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results; and
- If we are sending information relevant to your tenancy with us, your information may be disclosed to third parties responsible for facilitating distribution.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers, storage and processing outside the UK and Europe

We may transfer, store or process your information outside the UK and or European Economic Area (EEA) through the use of applications such as Dropbox and BoardBookit. By submitting your personal information you agree to this transfer, storage or processing.

Where information is transferred, stored or processed outside the UK or EEA we take all reasonable steps to ensure that there are adequate safeguards in place to protect your information in accordance with this notice.

Both Dropbox and BoardBookit comply with the EU-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and the EEA to the United States.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. All information you provide to us is stored on our secure servers, which are located within the UK, and our systems are protected with McAfee Endpoint Threatware (anti-virus, firewall, anti-spy and anti-malware).

Further information regarding this can be found in our Privacy and Openness and Confidentiality policies, both of which are available on our website or by request.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

A full schedule of the periods we will keep your information for can be found in our Document Retention Policy, which is available on our website or by request.

After the period specified in our Document Retention Policy your personal information will be destroyed if it is no longer required for the reasons it was obtained.

Your rights

You have the right at any time to:

Ask for a copy of the information about you held by us in our records;
Require us to correct any inaccuracies in your information;
Make a request to us to delete what personal data of your we hold; and
Object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at our registered address or via info@fifehg.org.uk

Fife Housing Group tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate.

If you have any further concerns regarding this, you also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
Email: scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.

Changes to this notice

This notice was last updated in May 2018 and will be kept under regular review. The most current version of this notice is available on our website or by request.

Appendix 3

Fife Housing Group is a trading name of Fife Housing Group Ltd and PACT Enterprises Ltd.

DATA SHARING AGREEMENT

between

Fife Housing Association Ltd, a Scottish Charity (Scottish Charity Number SC025647), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2476 R(S) and / or PACT Enterprises Ltd, Company Registration No.SC375254, both having their Registered Office at 7 Pitreavie Court, Pitreavie Business Park. Dunfermline. KY11 8UU ('the Group');

and

#[Insert organisation name, a # [e.g. Company] registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] ('**#[Party 2]**')]')

(each a '**Party**' and together the '**Parties**').

WHEREAS

(a) The Group and [*Insert name of party*] ('[Party 2]')intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the 'Agreement'); and

(b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement.

(c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of #[***insert details of relationship/ contract with Party 2***]

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out opposite:

'Agreement' means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

'Business Day' means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

‘Data’ means the information which contains Personal Data and Sensitive Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

‘Data Controller’ has the meaning set out in Data Protection Law;

‘Disclosing Party’ means the Party (being either the Group or #[Party 2], as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

‘Data Protection Law’ means Law relating to data protection, the processing of personal data and privacy from time to time, including:

(b) The Data Protection Act 1998;

(c) (with effect from 25 May 2018) The General Data Protection Regulation (EU) 2016/679;

(d) The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(e) Any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union;

‘Data Recipient’ means the party (being either the Group or #[Party 2], as appropriate) to whom Data is disclosed;

‘Data Subject’ means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1;

‘Data Subject Request’ means a written request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;

‘Disclosing Party’ means the party (being either the Group or #[Party 2], as appropriate) disclosing Data to the Data Recipient;

‘Information Commissioner’ means the UK Information Commissioner and any successor;

‘Law’ means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

‘Legal Basis’ means in relation to either Party, the legal basis for sharing the Data as described in Clause **Error! Reference source not found.** and as set out in Part 2;

‘Purpose’ means the purpose referred to in Part 2;

‘Representatives’ means, as the context requires, the representative of the Group and/or the representative of #[Party 2] as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;

‘Schedule’ means the Schedule in 6 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and

‘Security Measures’ has the meaning given to that term in Clause **Error! Reference source not found.**.

1.2 In this Agreement unless the context otherwise requires:

1.2.1 Words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:

(a) The Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;

(b) The General Data Protection Regulation (EU) 2016/679, in respect of processing undertaken on or after 25 May 2018; and

(c) In respect of processing undertaken on or after the date on which legislation comes into force that replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, that legislation;

1.2.2 More generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions,

consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;

2 DATA SHARING

Purpose and Legal Basis

2.1 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.

2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

2.3 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

Parties Relationship

2.4 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

2.4.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;

2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

2.4.3 it shall comply with its obligations under Part 6 of the Schedule;

2.4.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;

2.4.5 Provided that where the Data has been transferred outside the United Kingdom, the Disclosing Party may require that the Data is transferred back to within the United Kingdom:

(a) On giving not less than 3 months' notice in writing to that effect; or

(b) At any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom where it is being processed; and

2.4.6 It shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

2.5 The Disclosing Party undertakes to notify in writing the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

Transferring Data

2.6 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

3 BREACH NOTIFICATION

3.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):

3.1.1 The nature of the personal data breach or suspected breach;

3.1.2 The date and time of occurrence;

3.1.3 The extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and

3.1.4 Any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.

3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.

3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

4 DURATION, REVIEW AND AMENDMENT

4.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for #[***insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other***], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.

4.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.

4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:

4.3.1 The terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or

4.3.2 The Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.

4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.

4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:

4.5.1 Suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

4.5.2 Terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.

4.6 Where the Disclosing Party exercises its rights under Clause **Error! Reference source not found.**, it may request the return of the Data (in which case the Data Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain one copy for the purpose of complying with, and for so long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

5 LIABILITY

5.1 Nothing in this Agreement limits or excludes the liability of either Party for:

5.1.1 Death or personal injury resulting from its negligence; or

5.1.2 Any damage or liability incurred as a result of fraud by its personnel; or

5.1.3 Any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.

5.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses **Error! Reference source not found.** and **Error! Reference source not found.** above:

5.3.1 Each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;

5.3.2 Neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and

5.3.3 Use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

6 DISPUTE RESOLUTION

6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause **Error! Reference source not found.**, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

6.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause **Error! Reference source not found.**.

6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

7 NOTICES

7.1 Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting;

(iii) if by courier, the date and time the courier's delivery receipt if signed; or
(iv) if by fax, the date and time of the fax receipt.

8 GOVERNING LAW

8.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a **'Dispute'**) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

IN WITNESS WHEREOF these presents consisting of this and the preceding 6 pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

On behalf of the Fife Housing Group
At 7 Pitreavie Court, Pitreavie Business Park. Dunfermline. KY11 8UU

on
by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

_____

_____

On behalf of #[Party 2]

at

on

by

_____ _____

Print Full Name Director/Secretary/Authorised Signatory

before this witness

_____ _____

Print Full Name Witness

Address

_____

_____

_____

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN THE GROUP AND #[PARTY 2]

SCHEDULE PART 1 – DATA

Drafting Note: This Part should contain details of the Personal Data to be shared between Parties and will need to be populated on a case by case basis when utilising this Agreement.

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING

Purpose

The Parties are exchanging Data to allow #[insert details].

Legal Basis

#[**insert details - this will require specific requirements to be drafted in to the model Agreement depending on the relationship between the Group and Party 2**]

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient it can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of personal data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face
- Secure email
- Courier
- Encrypted removable media
- #[**insert further methods of transport of Data (and delete above if desired)**]

The data is encrypted, with the following procedure(s):

- #[**insert details**]

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

Fife Housing Group

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

#[Party 2]

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:

The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments [**Delete/amend as appropriate]**

The following additional measures are taken to ensure the security of any Data:

- Network username
- Network password
- Application username
- Application password
- Application permissions and access restricted to those who require it

[Delete/ amend as appropriate]

3 Disposal of Assets

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

SCHEDULE PART 6 – DATA GOVERNANCE

Data accuracy

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

Data retention and deletion rules

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.

Appendix 4

Fife Housing Group is a trading name of Fife Housing Group Ltd and PACT Enterprises Ltd.

DATA PROTECTION ADDENDUM

between

Fife Housing Association, a Scottish Charity (Scottish Charity Number SC025647), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2476 R(S) and / or PACT Enterprises Ltd, Company Registration No.SC375254, both having their Registered Office at 7 Pitreavie Court, Pitreavie Business Park. Dunfermline. KY11 8UU; ('the Group')

and

CONTRACTOR NAME, a # [insert type of business] registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] (the "Processor")

(each a "**Party**" and together the "**Parties**")

WHEREAS

(d) The Group and the Processor have entered in to an agreement/ contract to #[insert detail] (hereinafter the 'Principal Agreement'/'Principal Contract');

(e) This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (*delete as appropriate); and

(f) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/Contract shall remain in full force and effect. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **‘Applicable Laws’** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Group Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 ‘**Group Personal Data**’ means any Personal Data Processed by a Contracted Processor on behalf of the Group pursuant to or in connection with the Principal Agreement/Contract;

1.1.3 ‘**Contracted Processor**’ means Processor or a Sub-processor;

1.1.4 ‘**Data Protection Laws**’ means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 ‘**EEA**’ means the European Economic Area;

1.1.6 ‘**EU Data Protection Laws**’ means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 ‘**GDPR**’ means EU General Data Protection Regulation 2016/679;

1.1.8 ‘**Restricted Transfer**’ means:

1.1.8.1 A transfer of Group Personal Data from the Group to a Contracted Processor; or

1.1.8.2 An onward transfer of Group Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 ‘**Services**’ means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Group pursuant to the Principal Agreement/ Contract;

1.1.10 ‘**Sub-processor**’ means any person (including any third party and any , but excluding an employee of Processor or any of its sub-

contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Group in connection with the Principal Agreement/Contract; and

1.2 The terms, '**Commission', 'Controller', 'Data Subject', 'Member State', 'Personal Data', 'Personal Data Breach', 'Processing**' and '**Supervisory Authority**' shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3 The word 'include' shall be construed to mean include without limitation, and cognate terms shall be construed accordingly**.**

2. Processing of Group Personal Data

2.1 The Processor shall:

2.1.1 Comply with all applicable Data Protection Laws in the Processing of Group Personal Data; and

2.1.2 Not Process Group Personal Data other than on the Group's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Group of that legal requirement before the relevant Processing of that Personal Data.

2.2 The Group

2.2.1 Instructs the Processor (and authorises Processor to instruct each Sub-processor) to:

2.2.1.1 Process Group Personal Data; and

2.2.1.2 In particular, transfer Group Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and

2.2.2 Warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3 The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Group Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other

Data Protection Laws). The Group may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Group reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Group Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Group Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Group Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Sub-processing**

5.1 The Group authorises the Processor to appoint (and permit each Sub-processor appointed in accordance with this section 5 to appoint) Sub-processors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Sub-processors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Group prior written notice of its intention to appoint a Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. The Processor shall not appoint (nor disclose any Group Personal Data to) the proposed Sub-processor except with the prior written consent of the Group.

5.4 With respect to each Sub-processor, the Processor or the relevant shall:

5.4.1 Before the Sub-processor first Processes Group Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Group Personal Data required by the Principal Agreement;

5.4.2 Ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Sub-processor; and on the other hand the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Group Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 If that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Sub-processor; and on the other hand the Sub-processor, or before the Sub-processor first Processes Group Personal Data; and

5.4.4 Provide to the Group for review such copies of the Contracted Processors' agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the Group may request from time to time.

5.5 The Processor shall ensure that each Sub-processor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Group Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of the Processor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Group by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Group's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall:

6.2.1 Promptly notify the Group if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Group Personal Data; and

6.2.2 Ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Group or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Group of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 The Processor shall notify the Group without undue delay upon the Processor or any Sub-processor becoming aware of a Personal Data Breach affecting the Group Personal Data, providing the Group with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor shall co-operate with the Group and at its own expense take such reasonable commercial steps as are directed by the Group to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Group with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Group reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Group Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Group Personal Data

9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Group Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Subject to section 9.3, the Group may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Group Personal Data to the Group by secure file transfer in such format as is reasonably notified by the Group to the Processor; and (b) delete and procure the deletion of all other copies of Group Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.3 Each Contracted Processor may retain Group Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for

the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Processor shall provide written certification to the Group that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

10. Audit rights

10.1 Subject to sections 10.2 and 10.3, the Processor shall make available the Group on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Group or an auditor mandated by the Group in relation to the Processing of the Group Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Group only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3 Where carrying out an audit of Personal Data, the Group shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Group undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins

11. General Terms

Governing law and jurisdiction

11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

Order of precedence

11.3 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement/Contract in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement/Contract.

11.4 Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/Contract and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

11.5 The Group may:

11.5.1 By giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.5.2 Propose any other variations to this Addendum which the Group reasonably considers to be necessary to address the requirements of any Data Protection Law.

Severance

11.6 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

On behalf of the Fife Housing Group

At 7 Pitreavie Court, Pitreavie Business Park. Dunfermline. KY11 8UU

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

On behalf of the Processor

at

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

SCHEDULE

This is the Schedule referred to in the foregoing Data Protection Addendum between the Group and the Processor

Appendix 5

Document Retention Policy

Reference / Issue No:	G/11	3
Date of this version:	May 2018	
Next review due:	August 2021	
Lead responsibility:	Finance and Governance	
Contents:	30 pages	1 appendix

Contents:

1. Introduction

1.1 Storage space costs money. Maintaining an ever-growing set of paper files and archives held with external storage such as Iron Mountain takes up time and other valuable Group resources. Even where material is stored on computer (e.g. in our Filestream document imaging system), such a system will only be of value if it is manageable and accessible. What documents do we need to keep and for how long?

1.2 It would be impossible to list all the documents that the Group keeps. In many cases, it will be a matter of what 'feels right' for us and the exercising of common sense when making a decision on what to keep, what to archive or what to dispose of.

1.3 However, we need to keep in mind the need to comply with the General Data Protection Regulation (EU) 2016/679 (the GDPR) (see 3 below) and specifically its third principle, '*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'. Although not applicable in Scotland, the Group is guided by the Limitation Act 1980, which in many cases sets a five year retention period after an event has occurred. This can be after employment ceases (for employment records and personnel charts) or the resolution date for a whistleblowing event or termination of a contract with suppliers, agents etc.

1.4 The table below lists the principal documentation which the Group should keep, together with details of statutory retention periods and recommended retention periods. It is of course open to us to opt for longer periods if we choose because of a particular reason but this must be clear and consistent.

2. Storage medium

2.1 The medium in which documents are stored is largely a matter for us to determine, subject to any regulatory or statutory requirements. However, care should be taken to ensure that documents stored electronically will capture all the information on the document (front and back) and allow the information to be presented in a readable format and if necessary, be readily convertible to a paper format. Whilst we have recently purchased Filestream we should bear in mind that conversion of documents to paper form might require specific software and hardware. When such information systems are changed, conversion facilities need to be retained or otherwise remain available.

2.2 HM Customs and Excise has particular requirements relating to electronically stored data, and has the power to withdraw approval for such media in any individual case. Additionally, the original signed sheets of our tenancy agreements are required to be retained in original, paper format for presentation if ever required in a court of law and CaptureAll our selected document imagers are facilitating this as they scan a house file.

3. Data Protection

3.1 The **GDPR** will come into force on 25 May 2018. The core objective of the GDPR is to provide a framework in which the rights and freedoms of individuals can be protected. It also attempts to strike a balance between that requirement and the needs of organisations such as the Group to use information for the purposes of their business.

3.2 The GDPR is underpinned by six principles that need to be followed to ensure full compliance within the GDPR. They are:

1. Personal data shall be processed lawfully, fairly and lawfully in a transparent manner in relation to the data subject and in particular, shall not be processed unless specific conditions contained within the GDPR are met.
2. Personal data shall be obtained only for one or more specified, explicit and lawful legitimate purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive limited to what is necessary in relation to the purpose or purposes for which it is processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data shall not be kept in a form which permits identification of data subjects for longer than is necessary for that purpose or those the purposes for which it is processed.
6. Personal data shall be 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.

4. Group storage

4.1 Care must always be taken when deciding to store documents, whether that is physical storage such as with Iron Mountain, or it is scanning of documents into Filestream; both methods have a cost involved.

4.2 When considering the need for storage colleagues **must** consider:

Question	**Why it matters**
Do I need to access the documents?	If you send boxes for physical storage then have to request them back this can be very costly. If it's something you need to access then consider digital medium or retain the file.
Do we need to keep these	If we don't need to keep the items then don't. If

items and if so, for how long?	we do check the Appendix below to determine how long for.
Do I need the original version of this document or will a copy do in future?	If you know you will need an original then use physical storage or ensure that the required original sheets (e.g. signed tenancy agreements) are retained.
Do I know what's in the box I'm about to store?	If you aren't certain about what's in the box don't waste Group money by sending it for storage – only store that which is required
Have you decided whether it's best to physically store the documents or scan them?	These options have widely differing costs attached so you need to assess the best approach.
Does the document just stay in physical storage forever?	You need to determine the date for planned destruction and notify the storage company when storing initially. You will then be required by your manager to review the quarterly listing to agree which boxes can go for secure destruction; thus minimising our physical storage cost.

4.3 The lists of archived material will be review by the Business and Operational Team Leaders (BLT/OLT) on a quarterly basis and teams will take responsibility for ensuring the timely destruction of stored material which is no longer required.

4.4 It is vital that documents are not simply boxed and sent for storage because there has been a lack of attention towards reviewing the contents – this is a serious waste of resources and due to retrieval charges from the storage companies the costs of re-checking stored boxes is prohibitive.

4.5 Boxes are stored in a secure environment at Iron Mountain. Only authorised FHG colleagues can access the files and this is password protected. In addition, any lists received from Iron Mountain are also password protected.

5. Equality impact

5.1 There are no equality impacts relating to this policy.

6. Roles and responsibilities

6.1 The Board has ultimate responsibility to ensure that the organisation adheres to data protection legislation.

6.2 The Group's Director of Finance and Governance is responsible for this policy's review, implementation and proper application.

6.3 The Group's Business Support Manager is responsible for publishing, on a quarterly basis, to BLT/OLT, the Iron Mountain archive lists to ensure that destruction takes place in a timely and financially efficient manner.

6.4 All colleagues are responsible for ensuring that any documents put to storage, in any format, are done so in an appropriate manner and can confirm that their retention is necessary.

7. Performance management

7.1 Any concerns regarding the adherence to this policy will be reported to the Board.

8. Review

8.1 This policy is due to be reviewed every three years – or earlier if a material change or regulatory standard requires this.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
1. Governance				
Registration documentation (FHG as Community Benefit Society)	Permanently	CBSA	Permanently	CBSA
Certificate of Incorporation (PACT)	N/A	N/A	Permanently	Implied by CA, Sec.15.
Certificate of change of name (PACT)	N/A	N/A	Permanently	Implied by CA, Sec.80.
Memorandum and articles of association (original, rules, FHG and PACT)	N/A	N/A	Permanently	Best practice.
Articles of association (current, PACT)	Permanently	CA	Permanently	CA
Rules (current, FHG)	Permanently	CBSA	Permanently	Implied by CBSA, Sec. 18
Governance documentation for charitable status (FHG)	N/A	N/A	Permanently	Required for charitable status.
Constitution, aims and objectives used for charitable status (FHG)	N/A	N/A	Permanently	Required for charitable status.
Confirmation letter of charitable registration (FHG)	N/A	N/A	Permanently	Best practice.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
HMRC confirmation of charitable status	N/A	N/A	Permanently	Best practice
Certificate of registration with the Scottish Housing Regulator	N/A	N/A	Permanently	Best practice.
Board member documents – appointment letters, role descriptions, bank details etc.	N/A	N/A	6 years after board membership ceases	GDPR 5th principle CA recommendation for docs post termination of directorship - some details should be destroyed when membership ceases e.g. bank details etc.
2. Meetings (incl. AGMs)				
Notices of meetings	N/A	N/A	6 years	Re challenge to validity of meeting/resolutions.
Board and committee resolutions and minutes (PACT)	Permanently	CA	Permanently	Signed originals must be kept.
Board and committee resolutions, minutes and resolutions of Board (trustees) (FHG)	N/A	N/A	Permanently	Signed originals must be kept.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
3. Registrations and statutory returns				
Annual returns to the Scottish Housing Regulator, including annual returns on the Scottish Social Housing Charter	N/A	N/A	Permanently	Best practice.
Audited company accounts and financial statements and confirmation statements to the Register of Companies (PACT)	N/A	N/A	Permanently	Best practice
Audited accounts and financial statements and annual returns to the FCA (FHG)	N/A	N/A	Permanently	Best practice.
Declarations of interest	N/A	N/A	6 years	Limitation for legal proceedings.
Register of directors and secretaries (PACT)	Permanently	CA	Permanently	Implied by CA, Sec. 162 and 275.
Register of members and officers (FHG)	Permanently	CBSA	Permanently	FCA Implied by CBSA, Sec. 30.
Register of Shareholding members (PACT)	Permanently	CA	Permanently	Implied by CA, Sec. 113.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
				Records *may* be removed from register 20 years after membership ceases.
Register of seals	N/A	N/A	Permanently	Best practice.
Register of share certificates	N/A	N/A	Permanently	Best practice.
4. Strategic management				
Business plans and supporting documentation (e.g. organisation structures, aims, objectives, funding issues)	N/A	N/A	5 years after plan completion	Best practice.
5. Insurances				
Current and former policies	N/A	N/A	Permanently	Limitation can commence from knowledge of potential claim and not necessarily the cause of the claim. NCVO recommends 3 years after lapse.
Annual Insurance schedule	N/A	N/A	6 years	Best practice.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Claims and related correspondence	N/A	N/A	3 years after settlement	Zurich Municipal recommendation. NCVO recommends 3 years after settlement
Indemnities and guarantees	N/A	N/A	5 or 20 years after expiry of policy (20 years for land)	Limitation for legal proceedings.
Group health policies, e.g. Westfield Health, Occupational Health	N/A	N/A	12 years after cessation of benefit	Best practice
Employer's liability insurance certificate	N/A	N/A	40 Years	Employers' Liability (Compulsory Insurance) (Amendment) Regulations 2008removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims etc.
6. Finance, accounting and tax records				
Accounting records for Community Benefit Society	N/A	N/A	6 years from the end of the	Required by FCA and OSCR.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
or Charity (FHG)			accounting period to which they relate	
Accounting records (PACT)	CA, Sec, 388	6 years	6 years from the end of the accounting period to which they relate	TMA Sec.20. May require any documents relating to tax over 6 (plus) years.
Balance sheets and supporting documents	N/A	N/A	6 to 10 years from the end of the accounting period to which they relate	Best practice. To relate to accounting records.
Loan account control reports	N/A	N/A	6 years from the end of the accounting period to which they relate	Best practice.
(Scottish or Westminster) Government Housing	N/A	N/A	Permanently	Best practice.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Association Grant documentation				
Signed copy of report and accounts	N/A	N/A	Permanently	Best practice.
Budgets and internal financial reports	N/A	N/A	2 years	Best practice.
Tax returns and records	N/A	N/A	10 years from the end of the accounting period to which they relate	Best practice.
VAT records	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
Orders and delivery notes	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Copy invoices	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
Credit and debit notes	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
Cash records	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
Journal transfer documents	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Creditors, debtors and cash income control accounts	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
VAT related correspondence	6 years	VATA	6 years from the end of the accounting period to which they relate	Customs and Excise requirement for VAT registered bodies.
7. Other banking records				
Cheques	N/A	N/A	6 years from the end of the accounting period to which they relate	Limitation for legal proceedings.
Paying in counterfoils	N/A	N/A	6 years from the end of the accounting period	Limitation for legal proceedings.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
			to which they relate	
Bank statements and reconciliations	3 years from the end of the financial year the transactions were made	CA	6 years from the end of the accounting period to which they relate	Limitation for legal proceedings.
Instructions to bank	N/A	N/A	6 years from the end of the accounting period to which they relate	Limitation for legal proceedings.
8. Contracts and agreements				
Contracts under seal and/or executed as deeds	N/A	N/A	12 years after completion (including any defects liability period)	Limitation for legal proceedings.
Contracts for the supply of goods or services,	Duration of	PSCR	6 years after	Limitation for legal

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
including professional services	contract		completion (including any defects liability period) limitation for legal proceedings	proceedings. PCSR, Reg. 82 provides for the retention of executed contracts over €1m for at least the duration of the contract.
Contracts for works	Duration of contract	PSCR	12 years after completion (including any defects liability period)	Limitation for legal proceedings. PCSR, Reg. 82 provides for the retention of executed contracts over €10m for at least the duration of the contract.
Documentation relating to small one-off purchases of goods and services, where no continuing maintenance or similar requirement	N/A	N/A	3 years from the end of the accounting period to which they relate	Best practice. Suggested limit: goods or services costing up to £10,000.
Loan agreements	N/A	N/A	12 years after last payment	Best practice.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Licensing agreements, credit licence, music licence, etc	N/A	N/A	6 years after expiry	Limitation for legal proceedings.
Rental and hire purchase agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings.
Indemnities and guarantees	N/A	N/A	5 or 20 years after expiry of policy (20 years for land)	Limitation for legal proceedings.
Documents relating to successful tenders	3 years after award of contract	PCSR	5 years after the end of contract.	Recommendation of SFHA.
Documents relating to unsuccessful tenders	3 years after award of notification	PSCR	5 years after notification of unsuccessful tender.	Recommendation of SFHA.
Forms of tender	3 years after award of contract	PCSR	5 years after award / notification of end of contract.	Recommendation of SFHA.
Contract register	Permanently	PRSA	Permanently	PRSA, Sec. 35 requires this to

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
				be maintained.
Procurement strategy	N/A	N/A	6 years following expiry	Best practice.
Annual procurement report	N/A	N/A	6 years following expiry	Best practice.
9. Charitable donations				
Deeds of covenant	6 years after last payment	TMA	12 years after last payment	Limitation for legal proceedings if related to land.
Index of donations granted	N/A	N/A	6 years after last payment	Best practice.
Account documentation	3 years	CA	6 years	Best practice.
10. Application and tenancy records				
Applications for housing	N/A	N/A	5 years after offer accepted.	Recommendation of SFHA.
Recording forms for tenant profiling	N/A	N/A	None	Best practice in GDPR compliance requires form to be

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
				destroyed immediately statistics have been recorded on system.
Housing Benefit notifications	N/A	N/A	Duration of tenancy.	Recommendation of SFHA.
Rent statements, paper form or system	N/A	N/A	Permanently	Best practice.
Tenants' tenancy Files, including rent payment records, and details of any complaints and harassment cases	N/A	N/A	Duration of tenancy.	Recommendation of SFHA.
Former tenants' Tenancy Agreements, and details of their leaving	N/A	N/A	5 years post termination of tenancy.	Recommendation of SFHA. Any live issues for former tenant arrears will need to be kept until debt is cleared.
Care plans for children and related documents (where disclosed to FHG)	75 years	Ch A	Duration of tenancy.	Recommendation of SFHA.
Care plans for adults and related documents (where disclosed to FHG)	N/A	N/A	Duration of tenancy.	Recommendation of SFHA.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Documentation, correspondence and information provided by other agencies relating to special needs of current tenants	N/A	N/A	5 years post termination of tenancy	Information held on 'need to know' basis.
Medical and Social Services records liable to be confidential. To be returned or passed to subsequent agency at end of tenancy, or destroyed.	Records relating to offenders, ex-offenders and persons subject to cautions	N/A	5 years post termination of tenancy	While tenancy continues. Information held on 'need to know' and secure basis. Police sourced records may be confidential. To be dealt with as required by police.
11. Property records				
Rent determination documentation	N/A	N/A	6 years	Rent Officer recommendation.
Leases and deeds of ownership	N/A	N/A	While owned Deeds of title – until property disposed of. Leases – 15 years after expiry	Best practice. NCVO
Copy of former leases	N/A	N/A	5 years after lease	Recommendation of SFHA.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
			terminations.	Limitation for legal action relating to land or contracts under seal.
Wayleaves, licences and easements	N/A	N/A	12 years after rights given or received cease	Limitation for legal action relating to land or contracts under seal.
Abstracts of title	N/A	N/A	12 years after interest ceases	Limitation for legal action ceases relating to land or contracts under seal.
Planning and building control permissions	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal.
Searches	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal.
Property maintenance records	N/A	N/A	6 years after works undertaken	Limitation for legal action.
Reports and professional opinions	N/A	N/A	6 years after issue	Limitation for legal action.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Development documentation	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal.
Invoices	6 years	VATA	12 years	Limitation for legal action.
VAT documentation	See Finance, Accounting and Tax Records section	See Finance, Accounting and Tax Records section	See Finance, Accounting and Tax Records section	See Finance, Accounting and Tax Records section
Insurance	See Insurances section	See Insurances section	See Insurances section	See section on insurance.
12. Vehicles				
Mileage records	N/A	N/A	2 years after disposal	Best practice.
Maintenance records, MOT tests	N/A	N/A	2 years after disposal	Best practice.
Copy registrations	N/A	N/A	2 years after disposal	Best practice.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
13. Capital assets				
Capital Assets	N/A	N/A	6 years plus after date disposed of.	Best practice
Fixed Asset Register	CA, Charities Act	N/A	Permanently	CA, Charities Act
14. Employees: tax and social security				
Record of taxable payments	6 years	TMA	6 years	HMRC require retention of each payment for 3 years.
Record of tax deducted or refunded	6 years	TMA	6 years	HMRC require retention of each payment for 3 years.
Record of earnings on which standard National Insurance Contributions payable	6 years	TMA	6 years	HMRC require retention of each payment for 3 years.
Record of employer's and employee's National Insurance Contributions	6 years	TMA	6 years	HMRC require retention of each payment for 3 years.
NIC contracted-out arrangements	6 years	TMA	6 years	HMRC require
Copies of notices to employee (e.g. P45, P60)	6 years plus	TMA	6 years plus	HMRC require

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	current year		current year	
HMRC notice of code changes, pay and tax details	6 years	TMA	6 years	HMRC require
Expense claims	N/A	N/A	6 years after audit	Best practice.
Record of sickness payments	3 years following year to which they relate	SSPR	3 years following year to which they relate	HMRC require retention of each payment for 3 years.
Record of maternity payments	3 years following year to which they relate	SMPR	3 years following year to which they relate	HMRC require retention of each payment for 3 years.
Income tax PAYE and NI returns	3 years following year to which they relate	ITR	3 years after the end of the tax year related to.	Best practice.
Redundancy details and record of	N/A	N/A	6 years < 20 redundancies 12 years > 20 redundancies	Institute of Personnel payments and refunds and Development (IPD) recommendation.
HMRC approvals	N/A	N/A	Permanently	IPD recommendation

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Annual earnings summary	N/A	N/A	12 years	Best practice.
15. Employees: pension schemes				
Actuarial valuation reports	N/A	N/A	Permanently	IPD recommendation.
Detailed returns of pension fund contributions	N/A	N/A	Permanently	Best practice.
Annual reconciliations of fund contributions	N/A	N/A	Permanently	Best practice.
Qualifying service details	N/A	N/A	6 years after transfer or value taken	IPD recommendation.
Records relating to retirement benefits	6 years after year of retirement	RPS	6 years from the end of the tax year to which they relate	Statutory requirement.
16. Employees (personnel procedures)				
Terms and conditions of service, both general terms and conditions applicable to all colleagues, and specific terms and conditions applying to individuals	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Contracts for directors (companies)	3 years	CA	6 years after directorship ceases	Best practice.
Remuneration package	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings.
Former employees' Personnel Files	N/A	N/A	6 years	IPD recommendation.
References to be provided for former employees	N/A	N/A	20 years or until former employee reaches age 65 (whichever comes first)	Best practice.
Training programmes	N/A	N/A	6 years after completion	Best practice.
Individual training records	N/A	N/A	6 years after employment ceases	IPD recommendation.
Shortlists, interview notes and related application forms,	N/A	N/A	1 year	IPD recommendation.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Application forms of non-shortlisted candidates	Three months after notification	EA	6 months	Equality groups. 1 year limitation for defamations
Disclosure Scotland Protection of Vulnerable Groups (PVG) clearance documentation	Date of clearance and until next clearance check through disclosure checking where necessary			
Time cards and timesheets	N/A	N/A	2 years after audit	IPD recommendation.
Trade union agreements	N/A	N/A	10 years after ceasing to be effective	IPD recommendation.
Employer/employee committee minutes	N/A	N/A	Permanently	IPD recommendation.
Insurance claims	See Insurances section	See Insurances	See Insurances section	See Insurances section.
17. Employees: health and safety				
Medical records relating to control of asbestos	40 years	CAWR	40 years	CAWR
Health and Safety assessments	N/A	N/A	Permanently	IPD recommendation.

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Health and Safety policy statements	N/A	N/A	Permanently	Good practice.
Records of consultations with safety representatives	N/A	N/A	Permanently	IPD recommendation.
Accident records, reports	3 years after date of settlement	RIDDOR	3 years after date of last entry.	Limitation for legal proceedings.
Accident books	N/A	N/A	3 years after date of last entry.	Limitation for legal proceedings.
Sickness records	Three years after the end of each tax year for Statutory Sick Pay purposes. 6 years from end of sickness Limitation for legal proceedings.			
SSP (general) regulations	NCVO recommends 3 years.	However for industrial injuries not detectable within that period e.g. asbestos, the time period may be extended. Also for employees exposed to hazardous substances.		
Health and safety statutory notices	N/A	N/A	6 years after compliance	Limitation for legal proceedings
18. ASB				
ASB case files and associated documents	N/A	N/A	5 years or until end	

Appendix 1

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
			of legal action	
19. Residents' meetings, Scrutiny Group				
Minutes	N/A	N/A	1 year	GDPR

Key to statutory retention sources:

CA – Companies Act 2006

CAWR – Control of Asbestos at Work Regulations 2012

CBSA – Co-operative and Community Benefit Societies Act 2014

ChA – Children Act 1989

Charities Act – Charities and Trustee Investment (Scotland) Act 2005

EA – Equality Act 2010

GDPR – General Data Protection Regulation (EU) 2016/679

HMRC – HM Revenues and Customs

Income Tax (Pay As You Earn) Regulations 2003

LA /Limitations for legal proceedings – Limitation Act 1980

PRSA – Procurement Reform (Scotland) Act 2014

PSCR – Public Contracts (Scotland) Regulations 2015

RIDDOR – Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985

RPS – Registered Pension Schemes (Provision of Information) Regulations 2006

SMPR – Statutory Maternity Pay (General) Regulations 1986

SSPR – Statutory Sick Pay (General) Regulations 1982

TMA – Taxes Management Act 1970

VATA – Value Added Tax Act 1994

References:

- National Council for Voluntary Organisations (NCVO) guidance
- Scottish Federation of Housing Associations