LEVERN PROPERTY SERVICES LTD

Barrhead Housing Association Limited

1986-2016: Celebrating 30 years working in the community

Barrhead Housing Group Policy on:	**CO06a: Privacy Policy**

Compliant with Regulatory Standards	n/a
Compliant with Charter standards :	Standard 1: Equalities and 2: Communications
Guidance and Legislation	Data Protection Act 2018
Compliant with Tenant Participation Strategy :	n/a
Compliant with Equal Opportunities :	Commitments embedded within policy documentation
Equality Impact Assessment	NO EQIA is required in relation to this policy
Freedom of Information	Policy will be made available via BHG's Guide to Information
GDPR	Policy supports BHG's approach to GDPR, and the robust management of personal data
Compliant with Annual Assurance :	Yes
Linked Policies and Strategies	GDPR Policy Statement GDPR Privacy Policy GDPR Staff and Group Fair processing Notices

Date of Approval :	30 Jan 2020
Policy Review Date :	30 Jan 2023

Responsible Officer :	Chief Executive
Version History	Draft Approval: 30.01.2020 Last Approved : 2018

PRIVACY POLICY

Contents

1. Introduction
2. Data
3. Processing of Personal Data
4. Data Sharing
5. Data Processors
6. Data Storage & Security
7. Breaches
8. Data Subject Rights
9. Data Accuracy
10. Privacy Impact Assessments
11. Archiving, Retention and Destruction of Data
12. Responsibilities
13. Data Protection Officer

1. INTRODUCTION

Barrhead Housing Association recognises that the General Data Protection Regulation (GDPR) is an important piece of legislation (along with any subsequently enacted domestic data protection laws) to protect the rights of individuals and is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals.

The Association's staff members 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 Association needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that the Association has a relationship with. The Association 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 GDPR).

Barrhead Housing Association is the Data Controller under the legislation which means that it determines what purposes any personal information held, will be used for. It is also responsible for notifying the Information Commissioner's Office (ICO) of any issues arising in connection with the data it holds or is likely to hold, and the general purposes that this data will be used for.

This Policy sets out the Association's duties in processing that data where detailed procedures will also be produced separately for the management of such data.

2. DATA

2.1 The Association 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 Association is detailed within the individual Fair Processing Notices for customers and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

2.1.1 "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 Association.

2.1.2 The Association also holds Personal data that is sensitive in nature and this may include the 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".

2.1.3 Sensitive data is information relating to an individual's:

- *Racial or ethnic origin*
- *Political opinions*
- *Religious beliefs or other beliefs of a similar nature*

- *Whether they are a member of a trade union*
- *Their physical or mental health or condition*
- *Their sexual life*
- *A commission or alleged commission by them of any offence*
- *Any trial or sentence relating to any offence committed or alleged to have been committed by them*

3. Processing of Personal Data

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

- The individual has given their consent to the processing.
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Association'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 Association's official authority (currently only available to public authorites; or
- The processing is necessary for the purposes of a legitimate interest pursued by the Association or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the individual (this involves balancing the interests of the Association against those of the individual).

3.2. Fair Processing Notice

3.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by the Association. That 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.

3.2.2 The Fair Processing Notice sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's customers at the outset of processing their data.

3.3 Employees

3.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. 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.

3.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Chief Executive.

3.4 Consent

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

3.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association 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 courts are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest (currently only available to public authorities).

4. Data Sharing

4.1 The Association 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 Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

4.2 Data Sharing

4.2.1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data that the Association process as well. Both the Association and the third party will be

processing that data in their individual capacities as data controllers.

4.2.2 Where the Association 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 Agreement with the Association in accordance with the terms of the Association's policies.

5. Data Processors

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

For the Association this applies to services provided by our subsidiary, Levern Property Services which includes services for repairs, property factoring and housing support.

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

5.1.2 If a data processor wishes to sub-contact their processing, prior written consent of the Association 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.

5.1.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the Association's Data Protection Addendum

6. Data Storage and Security

6.1 Information and records relating to service users will be stored securely and will only be accessible to authorised employees. Information will be stored only for as long as it is needed or if required by statute and will be disposed of appropriately. We have a separate document retention schedule that sets out the retention periods for the various documents and information that the Association hold. It is Barrhead Housing Association's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6.2 Employees of Barrhead Housing Association are expected to follow the process outlined below regarding how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Champion or Data Protection Officer.

6.3 When data is stored on paper, it should be kept in a secure place to ensure that unauthorised people could not see it. These guidelines also apply to data

that is stored electronically but has been printed out by a staff member:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for example on a printer or in a public area such as reception or an interview room. Staff should follow the terms of the Associations' Clean Desk Policy at all times.
- Data printouts should be shredded and disposed of securely when no longer required.

6.4 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data and systems should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like CD, DVD or USB), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Association's standard backup and business continuity procedures.
- Personal Data should never be saved directly to laptops or other mobile devices such as smart phones or tablets.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Personal Data should be password protected when being sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the Association 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 the Association's Data Breach procedures

7.2 Reporting to the ICO

The Data Protection Champion or Officer 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 Information Commissioner's Office ("ICO") within 72 hours of the Association becoming aware of the breach . The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Subject Rights

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

8.2 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 Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice.

8.3 **Subject Access Requests**

All individuals who are the subject of personal data held by Barrhead Housing Association are entitled to:

- Ask what information the Association holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed about how the Association is meeting its data protection obligations

If an individual contacts the Association requesting this information, this is called a subject access request. The subject access procedure will be followed and the Data Protection Champion will take the lead in this process. A standard request form can be supplied, although individuals do not have to use this. The Data Protection Champion will ensure that the information is supplied within the timelines set out in the legislation, which is currently 1 calendar month. The identity of anyone making a subject access request will always be verified before handing over any information, in accordance with the SAR procedures;

8.3.1 The Association 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.

8.3.2 where the personal data comprises data relating to other data subjects, the Association 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,

8.3.3 In the event that consent is not provided to process a Subject Access Request, the Association will take reasonable steps to ensure the provided information is redacted, as necessary.

8.3.3 where the Association does not hold the personal data sought by the data subject, the Association 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.

8.4 **The Right to be Forgotten**

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

8.4.2 Each request received by the Association 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 DPC will have responsibility for accepting or refusing the data subject's request in accordance with legislation and the Association's policies

8.5 **The Right to Restrict or Object to Processing**

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

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

8.5.3 Each request received by the Association 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 DPC will have responsibility for accepting or refusing the data subject's request in accordance with the Association's policies and current legislation

9. Data Accuracy

9.1 Barrhead Housing Association will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition to having a Data Protection Champion with specific responsibility for ensuring compliance with Data Protection, Barrhead Housing Association will ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

10. Privacy Impact Assessments ("PIAs")

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

The Association shall 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; and in carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the 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. The Association 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 Champion 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 DPC within five (5) working days.

11. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the Association's Retention Schedule

12. Responsibilities

12.1 Everyone who works for Barrhead Housing Association has some responsibility for ensuring data is collected, stored and handled appropriately.

12.2 All teams that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

12.3 However, the following people have key areas of responsibility:

- The **Governing Board** is ultimately responsible for ensuring that Barrhead Housing Association meets its legal obligations.

- The **Director of Customer Services,** who for the purpose of this policy is the **Data Protection Champion,** is responsible for:

    - Reviewing all data protection procedures and related policies, in line with an agreed schedule

    - Arranging data protection training and advice for the people covered by this policy

- Dealing with requests from individuals to see any data that Barrhead Housing Association holds about them (this is known as a 'subject access request')

- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

- Liaising with any joint publicity ventures to approve any data protection statements attached to communications such as the newsletter or website

12.4 We, via our signed Contract Agreement with our IT support provider, will have systems in place to:

- Ensure all systems, services and equipment used for storing data meet acceptable standards

- Performing regular checks and scans to ensure that security hardware and software is functioning properly

- Evaluating these third-party services the Association is considering using to store or process data. For instance cloud computing services

13. Data Protection Officer

13.1 The Data Protection Officer's role is to assist the Association to monitor internal compliance, inform and advise on our data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

13.2 The DPO's tasks are as follows:

- to inform and advise the Association and its and employees about our obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).