****

**EMPLOYEE Fair Processing Notice**

(How we use employee information)

**Introduction**

The purpose of this notice is to explain to you the reasons which we will hold and use your personal data and explain your rights under the current data protection laws.

As your employer we will collect and process personal data relating to you to manage our contract with you. We are committed to being transparent about how we collect and use your data, and to meeting our data protection obligations with you.

This notice does not form part of your contract of employment or engagement with us. It applies to all our employees, ex-employees, workers, agency workers; apprenticeships, volunteers and consultants, regardless of length of service, and may be amended at any time. If any amendments are required in the future, we will notify you as is appropriate.

**Barrhead Housing Association (**including Levern Property Services) (referred to as the Group) are committed to a policy of protecting the rights of individuals with respect to the processing of their personal data and adhere to guidelines published in the Data Protection Act of 1998 and the General Data Protection Regulation (GDPR) (EU) 2016/679 applicable from 25th May 2018, together with any domestic laws subsequently enacted.

We are registered as a data controller with the Office of the Information Commissioner and our registered number is **Z1351301** and we are the data controller of any personal data that you provide to us. .

Our Data Protection Champion is Lorraine Dallas, Director of Customer Services, contact lorrained@barrheadha.org

Our Data Protection Officer is Iain MacLean, Corporate Services Manager at iainm@barrheadha.org

Any questions relating to this notice and our privacy practices should be sent either of the above Officers

**How we collect information from you and what information we collect**

This section sets out details of:

1. how information is collected and where personal information comes from (e.g. via website, Facebook; third parties, from information provided by the individual etc.);
2. the personal information collected from individuals; and
3. the reasons for collecting this information. We will specify whether this is collected by the data controller directly or received from third parties (where possible details of the third parties have been included).

**Where does your personal information come from?**

We may collect this information in a number of ways which include:

* Recruitment processes including information obtained from agencies
* Your identification documents you have given us
* Background checks conditional for your engagement with us
* PVG/Disclosure/DVLA checks relating to criminal convictions/offences
* Former employers or other individuals whom you have given us permission to contact to provide us with a reference. This data will include:
	+ - Your work history with them, including your dates you were with them,
		- the work tasks you did,
		- your level of responsibility,
		- job title,
		- salary on leaving,
		- reason for leaving their workplace and
		- whether they would be happy to have you work for them again.
* Medical professionals provide us with appropriate health information in order that we can manage any health- related situations that may have an impact on your ability to work with us.
* Professional bodies that confirm membership qualifications/training provide us with details of your attendance; qualifications attained; the location of any external attendance/and/or duration of relevant qualification/training.
* Our IT Service & Support Provider will, on request, provide us with the following personal information: Web browsing history; email exchanges; but only if we have a reason to monitor this information. This information will/will not be monitored routinely.

**What Information do we collect?**

The organisation controls and processes a range of information about you. In this notice ‘your personal information’ means your personal data i.e. information about you from which you can be identified. Your ‘personal information’ does not include data where your identity has been removed (anonymous data). It is really important that your personal information that we hold and process is accurate and up to date. Please keep us informed if your personal information changes during your engagement with us.

This includes:

* Your name
* Address
* Contact details including email address and telephone number
* Date of birth
* Gender
* The terms and conditions of your employment or engagement with us
* Details of your qualifications, skills, experience and work history, including start and end dates with previous employers and workplaces
* Information about your remuneration, including entitlement to benefits such as, pay, pension and holidays
* Details of your bank account and national insurance number
* Information about your marital status, next of kin, dependants and emergency contacts
* Information about your nationality and entitlement to work in the UK
* Information about any criminal convictions if relevant for your job.
* Details of your work pattern (days of work and working hours) and attendance at work
* Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals
* Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
* Assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence
* Information about medical or health conditions, including if you have a disability for which the organisation needs to make reasonable adjustments – that you have divulged to us
* Equal opportunities monitoring information about your ethnic origin, sexual orientation and religion or belief
* Photographs and videos
* Next of kin/Emergency Contact Details
* Details of Children (to process childcare vouchers)

The data we hold on you will be stored within the UK and EEA. The duration of how long we hold this information is contained within our Group Data Retention Policy.

**Photographs**

There will be instances where we will take photographs of employees for use in our publications and on our website. We will not assume staff consent, and from January 2020 we will always seek permission to use staff’s photographs before they are used for such purposes.

**Processing Personal Data**

As an organisation we will process data in accordance with the following legal grounds:

***Our Contract with you:***

We need to process the data we hold on you in order that we comply with our obligations with you under the contract we have with each other. This includes;

* the need to process your data to provide you with an appropriate contract,
* to pay you in accordance with your employment contract and
* to administer your employment benefits.

***Legal Obligations:***

We are required;

* to obtain check’s regarding your right to work in the UK,
* to deduct tax, National Insurance, and administrate your pension,
* to comply with health and safety laws and
* to enable you to take periods of leave to which you are entitled.

We are also required to process special categories of personal data, such as information about health or medical conditions to carry out our employment law obligations, such as those in relation to any disability you may have or arises.

***Legitimate Interests:***

We are also required to process your data in accordance with our legitimate interests which can occur, during and after our employment relationship which will allow us to:

* Maintain accurate and up to date employment records, contact details, emergency contact details, and records of employee contractual statutory rights
* Operate and keep a record of disciplinary and grievance processes,
* Plan for career development, succession planning and workforce planning
* Operate and keep a record of absence management procedures, to allow workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
* Obtain occupational health advice, ensuring that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled.
* Operate and keep a record of other leave you may take including maternity, paternity, adoption, parental and shared parental leave, to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
* Ensure effective general HR and business administration
* Provide references on request for current or past employees; and
* Respond to and defend against legal claims
* In the event of a business sale/transfer
* Any regulatory checks and/or statutory check/requirements in relation to your engagement with us
* Update our media platforms and issue publications confirming who our members of staff are.

**Processing Special Category Personal Data**

Special categories of information means information about your racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions, offences or alleged offences; genetic data; or biometric data for the purposes of uniquely identifying you. There are specific legal reasons for processing this special data are summarised as follows. Further information can be found on the ICO website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

(a) is carried out with the data subject’s explicit consent;

(b) is necessary for a legal obligation in the field of employment law;

(c) is necessary to protect the vital interests of the data subject or another person where the data subject is unable to give consent;

(d) is carried out by a non-profit-seeking body and relates to members of that body or persons who have regular contact;

(e) relates to data made public by the data subject;

(f) is necessary for legal claims;

(g) is for reasons of substantial public interest under EU or Member State law;

(h) is necessary for healthcare reasons;

(i) is necessary for public health reasons; or

(j) is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on EU or Member State law (Article 9 GDPR).

We collate the following special category data:

1. ethnic background for the purposes of collating and reporting on employment data to our Regulator
2. religious beliefs for the purposes of acknowledging, respecting and observing any special requirements as a result of those beliefs
3. health data that you have divulged to us for the purposes of any workplace considerations that we need to make, or if this falls within the interests of public health
4. criminal records for the purposes of ensuring that necessary background checks are made when recruiting for posts which involve vulnerable client groups.

**Employee Monitoring**

We will carry out necessary monitoring exercises if we have been made aware/or suspect that an employee is not adhering to the requirements as contained within our Group Internet & Electronic Communications Policy.

**Access to Data and Security**

***Access to Data***

In order to process your data in accordance with the grounds stated above the following will have access to your data, appropriate to the needs of that access, which could include:

Internally:

* Line manager
* IT staff
* Managers in the business area you work
* HR function

Third parties:

* For the purposes of pre-employment checks; past employers, disclosure and PVG
* For the purposes of processing data on behalf of us: payroll provider, Seeking advice in relation to your contract of engagement and other associated policies and procedures; pension administration, IT provider
* Any other third parties as necessary to comply with your contract of engagement and our legal and statutory obligations with third party organisations.

***Security***

When you give us information we take steps to make sure that your personal information is kept secure and safe.

It is therefore important that your personal information is stored securely and appropriate technical measures are taken to protect this information. This section sets out details of the security measures in place.

Any Information and records relating to individuals 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 Group hold.

It is our 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.

All employees of the Group 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 Officer or Champion.

When data is stored on paper, it should be kept in a secure place to ensure that unauthorised people could not see it. Staff should follow the Association’s Clean Desk Policy at all times.

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.
* Group 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.
* Data printouts should be shredded and disposed of securely when no longer required.

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.
* 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.

**Your Rights**

As a data subject, you have a number of rights, as follows:

* To be informed of the personal data we hold on you
* Access and obtain a copy of all your personal data on request
* Require the organisation to change incorrect or incomplete personal data
* Require the organisation to delete or stop processing your personal data e.g. where the data is no longer necessary for the purposes; and object to the processing of your data where the organisation does not require to process it
* To personal data portability
* To object to the personal data we hold on you
* To be informed of automated decisions made in relation to you

If you would like to exercise any of the above rights, please contact our Data Protection Officer Champion, Lorraine Dallas by email at lorrained@barrheadha.org

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: 0303 123 1115

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.

**Data Retention**

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including to satisfy any legal, accounting or reporting requirements.

We will retain all of your personal information during your engagement. After termination our policy on Data Retention clearly outlines what we will keep for former employees and for how long, to allow us to establish, exercise or defend legal claims, with the exception of the following:

* We will delete **out-of-date** contact, emergency contact, and bank account details whenever you provide us with updated details.
* We will retain **current** contact and bank account details during your engagement, and delete these when we have processed the final payment to you following the termination of your engagement.
* We will retain **current** emergency contact details during your engagement, and delete these when your engagement terminates.
* We will retain payroll and wage records, salary and benefits details, including pension and bonus details during your engagement as specified within our Group Data Retention Policy and/or where we are legally required to retain information.
* We will retain a copy of your driving licence/Insurance document during your engagement if required for the purposes of your role and delete this when your engagement terminates

**If you do not wish to provide your personal data**

You have obligations under your employment contract to provide the Group with the necessary data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights

Certain information, such as contact details, your right to work in the UK and the payment details, have to be provided to enable the organisation to enter into a contract of employment with you. If you do not provide other information, this will hinder the organisation’s ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

**Automated Decision Making**

No decisions are based solely on automated decision making.