

Policy	Data Protection Policy
Reference	G.05
Date Approved	May 2018
Review Date	May 2021



Terms Of Reference

- General Data Protection Regulation
- Data Protection Act 2018
- Equalities Act 2010
- ICO Guide to the General Data Protection Regulation
- SFHA Data Protection & Privacy Briefing (June 17)
- EVH Data Protection Information Note (July 2014)

Linkage to Internal Management Business Plan

To ensure that the work of the Association is supported by effective governance, financial and administration systems and that staff and Committee are accountable for the work of the Association.

Risk Factor

- Risks if:
- Improper conduct/inappropriate access to information
 - Breach of trust/confidentiality
 - SHR Engagement
 - ICO Intervention/Fine
 - Requests from data subjects imposing an unreasonable burden on the Association

Financial/Budgetary Implications

Cost of resources to ensure compliance
 ICO & Regulatory Fines for non-compliance
 Awards of compensation to aggrieved data subjects.

Contents

1. Introduction
2. Regulatory Standards & Legislative Framework
3. Equality & Diversity
4. Aims of Policy
5. Openness & Confidentiality
6. Registration & Responsible Person
7. Security & Risk Management
8. Employment Records
9. Obtaining Consent from Data Subjects
10. Joint Working/Sharing Of Information
11. Requests for Information from Data Subjects
12. Complaints
13. Monitoring & Review

1. Introduction

The Association stores information both on computer and within manual files. We recognise that the General Data Protection Regulation (GDPR) and Data Protection Act 2018 are important pieces of legislation to protect the rights of individuals in respect of any personal data that we keep about them, whether on computer or in manual systems. The Association also recognises the need to be open, transparent and accountable and to balance the rights of access and other rights contained within the GDPR with the rights of privacy and confidentiality.

The principal aim of the GDPR is to protect the right of privacy of the individual citizen against the misuse of personal data by organisations and seeks to restrict the flow of personal data.

The GDPR requires those who record and use personal data to be open and transparent about their use of that information and to develop sound practices. The GDPR contains 6 principles which regulate the way data can be collected, handled and used.

In practice all Registered Social Landlords (RSLs) and their residents and prospective residents are affected by the GDPR. All RSLs are subject to the duties under the GDPR and must register with the Information Commissioner and the pay an annual fee.

The rights and duties set out in the GDPR are designed to apply generally, but there are some exemptions from the GDPR contained within the Data Protection Act 2018 to accommodate special circumstances.

2. Regulatory & Legislative Framework

Standard 2 of the Regulatory Standards of Governance and Financial Management states:

“The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.”

Specifically relating to this Data Protection Policy Standard 2.2 states:

“The governing body recognises it is accountable to its tenants, and has a wider public accountability to the taxpayer as a recipient of public funds, and actively manages its accountabilities. It is open about what it does, publishes information about its activities and, wherever possible, agrees to requests for information about the work of the governing body and the RSL.”

Standard 5 states:

“The RSL conducts its affairs with honesty and integrity.”

With this in mind, Pineview Housing Association Limited stores personal data both on computer and within manual files and has registered all data processing information with the Information

Commissioner. The Association is registered as a fee payer with the Information Commissioner's Office. The register entry can be viewed at <http://ico.org.uk>.

The Association will ensure that our practices in the handling of personal data is fair, transparent and lawful and complies fully with the GDPR.

3. Equality & Diversity

The Association seeks to promote and achieve equality and diversity through the operation of an Equality and Diversity Policy, the requirements of which both in the letter and spirit will apply to this policy. In addition, the Scottish Social Housing Charter outlines the standard that our customers can expect in terms of equality:

- *every tenant and other customer has their individual needs recognised, is treated fairly and with respect, and receives fair access to housing and housing services.*

4. Aims of the Policy

To ensure members, tenants, sharing owners, owners and any other interested parties have access to information on how the Association conducts itself unless the information is considered commercially sensitive or personally confidential.

To ensure that the Association meets its obligations in respect of the GDPR and the Data Protection Act 2018.

To ensure that staff, committee, members, tenants and others are aware of their rights and obligations under the terms of the Act.

5. Openness & Confidentiality

Prior to going on to the terms of the GDPR principles, it is important to set out how the Association will deal with issues of openness and confidentiality.

The Association will provide the following information to interested parties either in the form of Newsletters, Annual Reports etc or on request.

- Performance against operational targets
- How to become a member of the Committee or influence decisions in other ways
- Outcome of Performance Audit Assessments
- Policies and Procedures
- Non confidential Committee papers and minutes
- Annual Accounts and Audit Report

This list is not exhaustive and the Association will action any request for information within a reasonable timescale, unless it is prevented from doing so by reasons of confidentiality.

It is not possible to produce a definite list of all items considered confidential, however, the following are considered confidential and will at no time be divulged inappropriately.

- Personal confidential information on residents or members of their family
- Personal confidential information on staff

It is important to stress that details that could identify an individual will not be provided at Committee Meetings and that only staff who are authorised will have access to tenants' details.

Any breach of confidentiality, whether deliberate or inadvertent, will be dealt with seriously by the Association. The circumstances surrounding the breach will, of course, be taken into account but will be dealt with under appropriate disciplinary procedures for staff and Committee. In the case of staff this could result in a warning or dismissal and in the case of Committee members this could result in their being asked to leave the Committee.

6. Registration & Responsible Person

The Data Protection Officer (DPO) has overall responsibility for data protection within the Association and will assist in implementing the requirements of the GDPR by providing advice and support to all departments relating to compliance with the GDPR, disseminating information relating to the GDPR, and responding to requests from customers, for example, to access personal data we hold about them.

The DPO will also have specific responsibility for personal data held on employees. Staff will be informed about data protection issues and their rights to access their own personal data in the procedure note relating to this Policy.

Senior staff will ensure that personal data processed by their function is kept up to date and complies with the above principles.

All staff will have a responsibility to fully comply with the requirements of the GDPR and this policy and the DPO is not personally liable or responsible for complying with the GDPR. When involved in requesting information, staff will explain why the information is necessary, what it is to be used for and who will have access to it.

In terms of responding to requests for data, the Director will work with the DPO and will take responsibility for the passing on of data about employees, former employees, job applicants etc and will delegate authority to other staff for the passing on of all other data i.e. about tenants, former tenants, housing register applicants, etc in so far as it relates to their function.

7. Security & Risk Management

The Association recognises the possible consequences should we fail to adhere to the principles within the GDPR. These include being subject to an enforcement notice from the Information Commissioner's Office to bring our practices in line with the GDPR; being required to pay compensation to a data subject through the courts if damage has been caused by our failure to meet the Act; being issued with a penalty notice of up to €20m in the case of very serious breaches of the GDPR; and the reputational damage associated with a GDPR breach.

A risk assessment will be carried out annually to determine what security measures are in place to protect data.

All staff will be issued with passwords in line with the Association ICT Policy and advised of what access they have to various data, both manual and computerised.

The Association operates a robust ICT Policy & Procedures and incorporates internal systems for managing and maintaining the Association's ICT infrastructure.

Employees and Committee Members will be obliged to sign a confidentiality form and to agree to the measures agreed with respect to processing of data.

Staff will receive training on this Policy when it is reviewed and updated. New Staff will receive training on this Policy as part of their induction. An information and guidance note will be issued to all staff and regularly reviewed.

Staff who breach this policy and procedures will be subject to the Association's disciplinary procedures.

8. Employment Records

This Section of the Policy relates to records in relation to the following:

- Applicants (successful and unsuccessful)
- Former applicants (successful and unsuccessful)
- Employees (current and former)
- Agency workers (current and former)
- Casual workers (current and former)
- Contract workers (current and former)
- Volunteers
- Work Experience Placements

When recruiting for new staff, the Association will always identify itself in advertisements and will only ask for information that is relevant to the job application. The Association will provide applicants with a statement containing the information required by the GDPR, including what the Association uses the data subject's personal data for, who it will be shared with, how long it will be kept and the data subject's rights in relation to their personal data. Disclosure information will be requested as per our Disclosure Policy.

Committee and Employees involved in recruitment and selection will be made aware that notes that they make during interviews etc may be requested by the data subject. All notes will be collected by the Director and held in the recruitment file until the records are disposed of. Refer to Recruitment Policy and Procedures.

Equal opportunities data will be held for monitoring purposes and for providing information on this to the Scottish Housing Regulator in accordance with the Recruitment Policy and Procedures.

When asked to provide a reference for another employee, line managers and others should provide a copy of the reference to the Director for inserting into the employee's personal file. References provided on employees by Association staff will be held in their personal file but will not be disclosed to them. References provided on an employee from other employers may be disclosed to them if requested but the author will not be identified.

All employees, volunteers and work experience placements will have a personal file, which will be retained either in the Director's room in a locked filing cabinet and/or in a secure electronic file accessed only by the Finance & Corporate Services Officer, Housing Services Manager and Director.

- Personal Information Sheet
- Appointment Information
- Job Description
- Health And Sickness Record

- Staff Appraisal
- Disciplinary Action
- Pension
- Car Etc Details
- Educational Courses
- Salary Information and Reviews
- General

Each year the Finance & Corporate Services Officer will provide a copy of the personal information sheet which is held on them to each member of staff and they will be asked to confirm the accuracy of this information or add any further details or changes. It is the responsibility of the employee to advise of any changes that occur to personal details between these yearly updates and the Association will not be held responsible for any inaccuracy in the records held by the failure of the employee to do so.

The Finance & Corporate Services section will hold salary, TOIL, Trade Union, Pension and Bank Details for each employee and this information will be retained on the Association's IT system on a secure drive.

Copies of self-certification absence forms and doctors Fit Notes will be kept in the employee's personal file and a computerised record of sickness and absence will be held by the Finance & Corporate Services Officer. The purpose of this will be to monitor individual sickness absence and to provide statistics to the Committee and the Scottish Housing Regulator. These reports will not identify individuals. Documentation in relation to pregnancy and maternity leave etc will be copied to the Finance & Corporate Services Officer for use in calculating and reclaiming if appropriate SSP and SMP.

Line Managers will be provided with emergency contact numbers for their staff for use in case of an emergency.

Car details will be provided to all staff where appropriate for health and safety reasons as per our Personal Safety Policy.

Line Managers should ensure that any information they hold on an employee is either passed to the Director for inclusion in their personal file (see above for information to be retained in their file) or held securely e.g. supervision meeting notes etc.

Employees will be provided with a standard statement containing the required information under the GDPR with regard to the processing of their personal data by the Association. This will be reviewed and updated from time to time in accordance with legal requirements. Processing may involve the DWP, HMRC, Pensions Trust, Trade Union, Auditors, Scottish Housing Regulator and others as required. It should be noted that if a request from a Building Society or other loan company or another employer is made for information relating to an employee's income or for a reference, employees will be consulted prior to the Association providing the reference. Employees may also be asked from time to time to feature in Newsletters, Annual Reports etc. This is covered by a separate photo consent document.

Employees may access their personal file but should make a request in writing to the DPO in advance. The DPO will respond to the request within one month and will remove any information that is considered to be in breach of the GDPR prior to disclosure. The employee's personal data will usually be provided in electronic format, although the personal file may be viewed in the Director's office.

9. Obtaining Consent from Data Subjects

Before being able to carry out processing of data, we must have a legal basis under the GDPR to justify the processing, unless there is an exception.

One of the legal bases relates to the data subject having consented to the processing and the following sets out some examples of where we have obtained the consent of the data subject:

- A clause is contained in our Tenancy Agreement advising that we can process the data contained within the agreement and pass any information to other relevant agencies as noted in our Data Protection Policy.
- Housing Register Applicants are asked to sign a declaration that we can ask for previous tenancy information.
- Special Needs Tenants authorise that information can be given to their care provider.
- Job Applicants agree that we can apply for references on them and that we can use equal opportunities information for monitoring purposes.
- Employees agree that information on absences, toil, appraisals etc can be reported to the Committee.
- Employees agree that we can process information to the Pensions Trust, trade union, etc on their behalf.

10. Joint Working/Sharing of Information

If staff are asked for information and are unsure whether to give it out or not they should seek advice from the DPO, Finance & Corporate Service Officer, Housing Services Manager or the Director.

In terms of sharing information with the police, we have a protocol for this.

Only where it is not clear from this policy that information may be provided, should details be entered in the Data Protection Register. For example, where councillors and MSPs seek information on their constituents at their request, where representative bodies such as CAB have a Mandate to act on a tenant's behalf, where information is shared as part of a protocol etc this does not require to be entered.

11. Requests for Information from Data Subjects

Requests for information can be made by individuals of 12 years of age and above who are deemed by the Data Protection Act 2018 to have sufficient maturity to understand what it means to exercise the right. Evidence of identity must be provided before information will be disclosed.

Data subjects will be provided with the data requested within **1 month** of providing sufficient information to enable the required data to be located.

The Association may not ordinarily charge a fee, unless the request is excessive.

The type of information that may be given in response to a request is as follows:

- Whether personal data is being processed
- What data is being processed, why and to whom that data may be disclosed
- Copy of the data in an intelligible form

- Source of the data
- How long the data will be kept by the Association
- Data subjects rights, including the right to complain to the Information Commissioner's Office

Personal data will, however, be withheld in a number of different circumstances, including where it:

- could identify someone else who objects to being identified
- could cause serious harm to either the data subject or another person's health
- would help to prevent or detect a crime
- is confidential because it was provided in the context of a lawyer - client relationship
- shows any actions the Association intends to take against the data subject
- the Association has a legal obligation not to disclose

Details of Subject Access Requests should be entered into the Data Protection Register.

The GDPR also gives data subjects other rights in relation to the processing of their personal data:

- right of rectification of inaccurate or incomplete personal data
- right to erasure of personal data
- right to restriction of processing of personal data
- right to data portability
- right to object to processing of personal data in specified circumstances

12. **Complaints**

Where data subjects are dissatisfied with the way their GDPR rights have been dealt with by the Association, they can complain to the Information Commissioner's Office at <http://ico.org.uk/make-a-complaint/> or 0303 123 1113.

Where the Association has refused to provide the data subject with access to their record, or to correct or erase inaccurate personal data without proper reason and the data subject has suffered material or non-material damage, then the data subject can take legal proceedings in the courts against the Association for compensation.

Where data subjects are dissatisfied with the way their request for personal data has been dealt with and it falls outwith the scope of the GDPR, they should make a complaint in accordance with the Association's Complaints Policy. Ultimately, they may apply to the Public Services Ombudsman.

13. **Monitoring & Review**

The following will take place annually:

- Review of data held and clear down
- Newsletter article for tenants on data protection

The following will take place when the policy is reviewed:

- Training for staff and Committee
- Signing of Confidentiality Form by staff and committee

This Policy will be reviewed every three years unless there are legislative changes or other reasons for reviewing earlier.