

COR13	ADOPTED: 27.02.02	REVIEWED: 23.2.05; 27.2.08; 23.2.11; 26.2.14; 27.9.17 28.10.20
--------------	--------------------------	---

DATA PROTECTION POLICY

1.0 INTRODUCTION

This policy describes how we will seek to ensure openness and accountability in our activities, while maintaining the confidentiality of personal and sensitive details, including commercially confidential information.

This policy is supported by the Data Protection & Access to Personal Information procedures, which describes how we will respond to requests from individuals to access information we hold about them, under the Data Protection Act.

It should be read in conjunction with the following:

- Committee Members Code of Governance, section 6.2
- Committee Members Code of Conduct, section 4.13
- Staff Code of Conduct, sections 5.1 – 5.3
- IT System Security and IT Use and Communications policies.
- Freedom of Information and Environmental Information Regulations.

The Association must comply with the EU General Data Protection Regulations, referred to as (the) GDPR, effective from 25 May 2018 and the Data Protection Act 1998.

The GDPR applies to ‘personal data’ meaning any information relating to a living identifiable person who can be directly or indirectly identified by a personal identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

The GDPR has the concept of “special category” personal data. Under GDPR personal data in this category is: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

For the purposes of GDPR, children are classed as individuals under the age of 13. Children have the same rights as adults over their personal data.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Our duty relates to our dealings with:

- applicants, tenants and factored owners;
- our staff, committee members and other members of the public;
- all the local and national agencies and authorities which we currently deal with;
- all commercial contacts.

2.0 COMPLIANCE

The Association will only use personal data where strictly necessary and will rely on an appropriate lawful basis for processing personal data.

The Association will maintain registration with the Information Commissioner's Office referred to as (the) ICO, in accordance with the requirements of the GDPR.

The Association will have a dedicated Data Protection Officer (DPO).

All staff will receive necessary training in the operation of the GDPR as it relates to their specific duties, and in the maintenance of the confidentiality and security of the manual and computer information that we hold.

The Association will implement measures that meet the principles of data protection by design (designing projects, processes, products or systems with privacy in mind at the outset) and data protection by default.

The Association will use data protection impact assessments to help identify and reduce the data protection risks of its projects and meet individuals' expectations of privacy.

The Association will have reporting procedures in the event of a data breach or potential breach occurring.

3.0 OPENNESS

Our aim is to conduct our activities openly and to make information publicly available unless there are justifiable reasons for withholding it.

We will fully comply with legislation regarding making information available. This will include compliance with FOI and EIRS.

Prospect will make available a broad range of information in accordance with the Freedom of Information (FOI) and Environmental Information Regulations (EIRS).

4.0 CONFIDENTIALITY

4.1 Collecting and holding information

We recognise that:

- we need to collect and hold information about individuals – e.g. applicants, tenants, employees – and about the range of groups, external organisations, contractors and suppliers etc. that we deal with;
- we have a responsibility to ensure that all the information we collect is held securely and is only accessed and used by those employees who need to do so as part of their duties.

4.2 Manual records

Manual records containing information covered by the GDPR will be stored as detailed in the Data Protection Procedure, with access being restricted to those employees who require the information for their duties.

Keys for cabinets, cupboards etc. holding personal files will either be held by a specific post-holder or kept in a secure location accessible only by authorised employees.

4.3 Computer records

Personal and sensitive information held on computers will be stored and accessed as detailed in the IT System Security policy, with access being restricted to those employees who require the information to carry out their duties.

The approval of levels of access and the advice regarding passwords will be as described in the IT System Security policy and procedure.

4.4 Office security

The office will be locked and the alarm system set when no staff are present, and the alarm system will be linked to a central control station. Out with the publicised office opening hours, when employees are in the building:

- public access to the office will only be possible by arrangement;
- if there are less than two employees on the ground floor the main external security door will normally be locked, unless there is a meeting taking place in which case it may be left open with the glass door locked.

Visitors will not be permitted access to any part of the office past Reception unless invited by an employee who is then responsible for making sure that they do not have access to any personal information.

4.5 Requests to access data

As permitted by the GDPR and related statutory regulations, we will comply with requests for access to information we hold about individuals, so long as the request is from the individual concerned or someone authorised to apply on their behalf.

Requests will be dealt with as detailed in the Data Protection & Access to Personal Information procedure supporting this policy.

4.6 Sharing data with others

To comply with the GDPR we will not normally pass on information we hold to any other individual or organisation without the written permission of the person concerned. The main exceptions will be where the passing on of such information is:

- covered by an agreement, protocol or contract that complies with the principles of the GDPR, which has been entered into with third parties with whom our staff need to share information;

- permitted by law, e.g. where a Police investigation into criminal activity requires the divulging of information we hold, including where such a request is accompanied by a Court Order.

The Association does not permit the transfer of personal data outside the European Union. Additionally, the Association's data-sharing agreements with third-party organisations expressly forbids data processors transferring data that the Association controls outside the European Union.

We will ensure that any contract with a company providing a service includes a 'non-disclosure' clause covering any personal or sensitive data company staff may be given access to in the course of their work.

We will ensure that, apart from the exceptions described below, all reports to the Management Committee relating to applicants, tenants or employees are anonymous, i.e. that individual names do not appear.

The exceptions will be where identification is essential or unavoidable in the Committee's consideration of the matter, e.g. when hearing an employee's appeal against disciplinary action, or a tenant's attendance to appeal against a decision made by staff.

We will ensure that in making any information available to the media or other agencies, the anonymity of individuals is maintained, unless written permission is obtained in advance for names to be released or individuals to be identified.

4.7 Financial and other management information

We will apply the principles described above regarding personal and sensitive information to all financial and general management information.

In accordance with the Committee Members' Code of Governance and Code of Conduct, and our Committee Standing Orders, the proceedings of the Management Committee or Working Group meetings will be regarded by all present as being confidential.

The minutes of meetings that become the publicly available record, in addition to ensuring that individuals are not identified, will not include 'commercially sensitive' information, for example:

- the results of tendering exercises, where tenderer's names are linked to the amount of their bid – the name of the successful tenderer only will be minuted;
- financial details relating to agreements with lenders regarding loans to the Association – the name of the lender and amount borrowed will be minuted;
- details of claims against contractors or suppliers, or claims against the Association by them, particularly where such claims are subject to legal action, or details of disputes with contractors or suppliers before legal action is taken – a general reference to the matter will be minuted;
- details of discussions with the Scottish Housing Regulator regarding the financial position of the Association – a general reference to any meeting will be minuted.

4.8 Use of information, breach of confidentiality and subject consent

All information held by us will only be used for the purposes for which it has been obtained, or other legitimate purposes allowed by the GDPR. In particular, Committee Members and employees will not use any information obtained in the carrying out of their duties for personal gain, or pass any such information on to any other person who might use it in such a way.

Any breach of confidentiality by a Committee Member will be dealt with in accordance with the Committee Members Code of Conduct.

Any breach of confidentiality by an employee will be dealt with under our Disciplinary policy and procedures.

We recognise that individuals have the right to choose how they want their personal information to be used. We will have a variety of Fair Processing Notices to cover different aspects of our work. These will be publicised to our tenants and other service users.

4.9 Use of data for research purposes

If we are considering using personal data for research purposes, we will always consider whether it is necessary to process that data in order to achieve the research purpose. If such processing is necessary, then provided the data has been obtained fairly and lawfully it may be used for research purposes under the GDPR

We will use data collected for one piece of research for other research only with the consent of the data subject(s). We will ensure that there will be no direct consequences for the individuals who have taken part in the research, and that their personal data will not be processed in a way that could cause damage or distress to any data subject.

Wherever possible we will anonymise the names of research subjects so that individuals cannot be identified.

4.10 Retention of data

As part of the Data Protection Procedure we will have a data retention schedule that sets out the period of time that we will keep data for. This information, where appropriate, will be included in the relevant Privacy Notice.

When data is no longer required it will be disposed of securely as set out in the Data Protection Procedure.

5.0 IMPLEMENTATION AND REVIEW

The Director is responsible for ensuring that this policy is implemented as required by Committee Members and all staff.

The Association's Data Protection Officer, responsibilities include ensuring that all employees are kept up to date with current data protection regulations and good practice.

The Director will ensure that this policy is reviewed by the Management Committee at least every 3 years.

Reviewed by the Management Committee on 28 October 2020

Next review due by: October 2023

GDPR - Principles

The following principles are set out in the GDPR, and it is a requirement under Article 52 that they are followed by organisations.

- (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- (f) 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.

PROSPECT EQUALITY IMPACT ASSESSMENT RECORD

Title of policy/ practice/ strategy	Data Protection	
Department	Corporate	
Who is involved in the EQIA?	Brendan Fowler	
Type of policy/ practice/ strategy	New <input type="checkbox"/>	Existing <input checked="" type="checkbox"/>
Date completed	07/10/20	

Stage 1: Screening Record

What is the main purpose of the policy?

The policy sets out our approach to data protection, covering both legislation (current and future) and good practice.

Who will the policy benefit and how?

This policy affects anyone for whom Prospect holds personal information. This includes applicants, tenants, factored owners, suppliers and staff members.

For each equality group, does or could the policy have a negative impact?

Protected characteristic	Negative	Positive/no impact	Don't know
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Disability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gender reassignment	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Marriage & civil partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Pregnancy & maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Religion or belief (including no belief)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sex	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sexual orientation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

If you answered negative or don't know to the above question you should consider doing a full EQIA.

Are there any potential barriers to implementing the policy?

Barriers would relate to a lack of staff awareness. This will be tackled through staff involvement in the development of procedures, and staff training.

	Yes	No
Is a full EQIA required?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

If you answered no to the above question explain why a full EQIA is not required:

No impact on equalities identified:	<input type="checkbox"/>
Other:	

Stage 2: Data and evidence gathering, involvement and consultation

Include here the results of your evidence gathering, including qualitative and quantitative data and the source of that information, whether national statistics, surveys or consultations with relevant equality groups.

Source	Qualitative evidence provided	Quantitative evidence provided	Which protected characteristics are covered?	Gaps identified/ action taken
Management information data		Annual staff and committee equalities data	Age, disability, gender, ethnicity. In some cases other protected characteristics	Membership data not collected.
Tenant satisfaction survey		Survey carried out in 2019	Age, disability, gender, ethnicity. In some cases other protected characteristics	Data becoming out of date.
Committee, Equalities Working Group and Tenants Forum minutes	Equality related issues identified and discussed		Various	
Review of complaints received	Tenant/service user experience	Statistical data on types of complaint	All protected characteristics	
Observations/conversations (anecdotal)	Staff/committee/tenant/service user levels of understanding, inclusive practice		All protected characteristics	
Edinburgh Census 2011		Statistical data	Age disability, gender, ethnicity, marital status, religion or belief.	Data becoming out of date.
EdIndex data		Statistical data provided for individuals on the housing waiting list	Age, disability, gender, ethnicity. In some cases other protected characteristics.	Data becoming out of date.
SHR Annual Return on Charter data		Statistical data on staff, committee and tenant profile for RSLs	Disability, ethnicity.	

Stage 3: Assessing the impacts

How might the policy impact on people who share protected characteristics? Include both positive and negative impacts.

Protected Characteristic	Description of Impact
Age	Information on this characteristic is routinely collected and held on individual's record, and must be protected.
Disability	Information on this characteristic is routinely collected and held on tenant records, and must be protected.
Gender reassignment	Information on this characteristic is not routinely collected for tenants and applicants and where it is collected is not held on an individual's record, but rather in an anonymous way. This information can be held for staff and committee members, and therefore will need to be protected.
Marriage & civil partnership	Information on this characteristic is routinely collected and held on individual's record, and must be protected.
Pregnancy & maternity	Information on this characteristic is not routinely collected for tenants and applicants and where it is collected is not held on an individual's record, but rather in an anonymous way. This information can be held for staff and committee members, and therefore will need to be protected.
Race	Information on this characteristic is routinely collected and held on individual's record, and must be protected.
Religion or belief (including no belief)	Information on this characteristic is not routinely collected. When it is it is not held on an individual's record, but rather in an anonymous way.
Sex	Information on this characteristic is routinely collected and held on individual's record, and must be protected.
Sexual orientation	Information on this characteristic is not routinely collected. When it is it is not held on an individual's record, but rather in an anonymous way.

How does the policy promote equality of opportunity?

The information that we hold on the protected characteristics, whether anonymised or not, helps us to assess the services that we provide to ensure that there is equal access to protected groups. The policy allows us to continue collecting this information, but ensuring at the same time we comply with legislation and protect the information that we hold.

How does the policy promote good relations?

By holding the information we do, we can analyse trends to make sure that any concerning trends are identified and acted upon.

Stage 4: Decision making and monitoring

Identifying and establishing any required mitigating action

If, following the impact analysis, you think you have identified any unlawful discrimination – direct or indirect - you must consider and set out what action will be undertaken to mitigate the negative impact.

Does the assessment show a potential for differential impact on any group(s)?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Is there potential for unlawful direct or indirect discrimination?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

What arrangements could be implemented to reduce or mitigate any potential adverse or negative impacts identified?

None identified.

Describing how Equality Impact analysis has shaped the policy making process

The impact analysis has highlighted the importance of keeping information on the protected characteristics, led us to consider how we can do this whilst at the same time protecting this information.

Monitoring and Review

Any breaches of this policy will be monitored, and any equalities issues related to this considered. The policy will be reviewed every three years by the Director.

Stage 5 - Authorisation of EQIA

Please confirm that:

- ◆ This Equality Impact Assessment has informed the development of this policy:

Yes No

- ◆ Opportunities to promote equality in respect of age, disability, sex, pregnancy and maternity, gender reassignment, sexual orientation, race and religion or belief have been considered, i.e.:
 - Eliminating unlawful discrimination, harassment, victimisation;
 - Removing or minimising any barriers and/or disadvantages;
 - Taking steps which assist with promoting equality and meeting people's different needs;
 - Encouraging participation (e.g. in public life)
 - Fostering good relations, tackling prejudice and promoting understanding.

Yes No

Declaration

I am satisfied with the equality impact assessment that has been undertaken for **Data Protection Policy**.

Name: Brendan Fowler

Position: **Director**

Authorisation date: 7 October 2020