Hanover (Scotland) Housing Association

First Line Data Protection Handbook

Version: 1.1

Published October 2019

Document Control

File Name	Front Line Data Protection Handbook
Original Author(s)	Rob Horne

Version	Date	Author(s)	Notes on Revision
1.0	25 January 2019	Rob Horne	Initial version
1.1	October 2019	Susan Campbell	Reviewed

Review

This policy shall be reviewed annually by the Data Protection Officer and amended as appropriate to reflect any changes to the requirements for the use of Hanover (Scotland) Housing Association's information assets or changes to Regulations for storage or processing of personal data. Amendments to the policy will be approved by the Chief Officers. The following table provides a record of these reviews:

Date	Reviewer	Approver	Actions
October 2019	Susan Campbell	Adam Curry	Reviewed

Distribution List

Name	Comment
All staff	Distribute to staff at induction and after updates
Interested parties (e.g., third party suppliers or regulators)	Only distribute with authorisation from the DPO

1. GUIDANCE

Hanover (Scotland) Housing Association collects the personal information of people we come into contact with. This document provides high level information for all staff on their responsibilities for handling personal data, and any requests or incidents which they have responsibility to handle, and contains references to more in depth documentation.

All documents **referenced in bold** can be found on the Hub.

When we collect, store or use (collective called "processing") personal information we must follow eight rules:

1.1. WE CANNOT PROCESS A PERSON'S DATA WITHOUT A LEGAL REASON TO SO

The Data Protection Act 2018 which incorporates the GDPR sets out a number of defined legal bases for processing personal data. More information on the legal bases under which we process personal data can be found throughout the **Data Protection Policy** where we also commit to observing all statutory and common law requirements and uphold expectations of ethical conduct (**Section 4**).

1.2. WE NEED TO TELL PEOPLE EXACTLY WHAT WE'RE DOING WITH THEIR INFORMATION

When processing personal data, we're required by law to tell people what's happening with it. Further information is available in our **privacy policies**, which tell people why we collect their personal data, how we will use it, how long we will keep it and if we share it with anyone else.

1.3. WE MUSTN'T PROCESS MORE OF SOMEONE'S INFORMATION THAN WE NEED TO

We must try to minimise the amount of personal data we process, so if we only need a name and phone number, we shouldn't also ask for their address, DOB or anything else. Particularly sensitive data, such as data relating to health and religion, and children's data, must only be processed under certain conditions. **Section 3 of the Data Protection Policy** has more information on what personal data is and special categories of data and includes our commitment to paying particular regard to constraints on the processing of special categories of data (**Section 4**).

1.4. PEOPLE'S INFORMATION MUST BE KEPT SECURE

It is important we protect people's information from being stolen, modified, deleted or adversely affected in any other way. The **Data Classification Policy** contains information on how to classify and handle personal data. **Section 7 of the Data Protection Policy** lists good practice for keeping personal data secure. Our **Information Security Policy** explains your responsibilities for protecting

information (**Section 7**), including familiarising yourself with and complying with the contents. If you suspect a breach has occurred, the **Incident and Breach Policy** contains further information on what to do, including how to identify a potential breach.

1.5. THE INFORMATION WE PROCESS NEEDS TO BE ACCURATE

Inaccurate personal information can have a negative effect on a person, which can range from not receiving a letter to being given the wrong care. It's important the personal data we collect is accurate and kept up to date. Depending on the service we supply we will periodically check for accuracy and encourage our residents to tell us when something changes.

1.6. ONCE WE NO LONGER NEED THE INFORMATION, WE MUSTN'T CONTINUE TO KEEP IT

If we have no need of someone's personal data, then we no longer have a legal reason to keep it. We must remove the data, usually by deleting it or by changing it so it becomes anonymous and cannot be linked to that person again. **Section 9 of the Data Protection Policy** contains information on how we manage retention of personal data, including information on what must be recorded in our **Information Asset Register**. Retention schedules are in our **Data Retention Policy** and the **Data Retention Procedure** explains how to implement them.

1.7. IF A PERSON ASKS ABOUT THEIR DATA, WE MUST ANSWER THEM

Everyone whose personal data we process has a number of legal rights, such as asking us what information we hold about them. **Sections 6 and 10 to 17 of the Data Protection Policy** explains the rights of individuals in respect of their personal data and what to do if you receive a request, commonly referred to as a Data Subject Access Request (DSAR or just SAR).

1.8. WE MUST ALWAYS BE ACCOUNTABLE FOR HOW WE USE PERSONAL INFORMATION

Wherever we process people's personal data we must make sure we comply with all the above and apply the same care and attention to our suppliers and service providers.

Our **Information Risk Management Policy** describes how we identify and manage the risks we face when processing data and how we assign an owner for information assets who is responsible for their security. Our **Information Security and Risk Management Framework** sets out how we inform staff, tenants and other interested parties about information security, managing risks and their responsibilities in these areas.

The **GDPR Requirements for Tendering** explain how we address the requirements for processing personal data in tender documents, and the **Supplier Management Policy** describes the process for managing the risks we could face from services provided by third parties.

2. FURTHER INFORMATION

If you have any questions about the content or operation of the **Data Protection Policy**, the GDPR, or any other data protection policy or procedure, or if you have any concerns that any policy is not being or has not been followed by Hanover Personnel, please contact the DPO. Our **Data Protection Policy** also lists occasions when you must always contact the DPO.