Our approach to GDPR v2

Our policy to using personal data with integrity.

The basics

The UK General Data Protection Regulation, or GDPR for short, is a law consisting of rules for how organisations and companies must use personal data with integrity and in a non-harmful way. Personal data is any information that could directly or indirectly identify a living person.

This policy outlines our obligations for the protection of personal data and the rights of our customers and colleagues in compliance with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and how we comply with the Privacy and Electronic Communications Regulations (PECR). It sets out how we comply with GDPR to make sure all personal data is collected, processed, transferred, stored, and disposed of correctly.

Our approach

To make sure that we comply with GDPR and ensure that we use data lawfully and with integrity. We must:

- Process it lawfully, fairly and in a transparent way.
- Only collected it for specific and legitimate reasons.
- Limit collection to what is necessary for our intended purpose.
- Keep customers informed of the purposes for which we use their data.
- Take reasonable steps to make sure any inaccurate data is erased or corrected without delay.
- Keep our data only for as long as necessary and make efforts to remove data which is no longer needed.
- Process and store personal data in a way that ensures it's kept as securely as possible.

Lawful Bases for Processing

We must make sure that we comply with GDPR and ensure that we use data lawfully and with integrity. We process personal data under the following lawful bases:

- **Contract** – to manage tenancies, repairs, and services
- **Legal obligation** – e.g., health and safety compliance, regulatory reporting
- **Legitimate interests** – e.g., preventing fraud, improving services
- **Consent** – for optional communication (e.g., newsletters)s
- **Vital interests** – emergencies affecting the health or safety of tenants
- **Public Task** – Processing necessary to perform a task carried out in the public interest

Types of personal data we collect

- Contact details (name, address, phone, email)
- Tenancy and housing application information
- Income, benefits, and employment details
- Rent payment history
- Health or vulnerability information (special category data)
- CCTV images and call recordings
- Repairs and maintenance records

Special category data is processed only under allowed conditions (e.g., substantial public interest, employment obligations).

We also process information relating to criminal convictions, offences, or alleged offences. This type of data is governed separately and is not treated as special category data, but it is subject to similarly strict safeguards.

Data Protection by Design and by Default

We are committed to embedding data protection into all systems, processes, and services from the earliest possible stage. We ensure that privacy and data protection principles are built into the design of our housing, tenancy, digital, and customer-facing services.

Data Protection Impact Assessments (DPIA's)

We will carry out Data Protection Impact Assessments (DPIAs) where required under Article 35 UK of the UK GDPR when introducing or changing any process, system, or projects that may involve high-risk data processing.
Examples include:

- Introducing new housing management software
- Implementing CCTV or audio recording
- Using new contractor or maintenance platforms
- Processing large amounts of sensitive or vulnerability data

A DPIA will:

- Identify risks to individuals
- Assess their likelihood and severity
- Identify measures to mitigate each risk
- Record outcomes and approval decision

No high-risk processing will commence until the DPIA is approved by the Data Protection Officer (DPO).

The project lead will identify the need for a DPIA by using the ICO DPIA screening template. If a DPIA is required, the project lead will complete the DPIA template and list mitigations for any risks identified.

This will be reviewed by the Data Protection Officer who will assess to see if the level of risk is acceptable and the mitigations highlighted are adequately addressed. If there are any high risks identified the DPO will contact the Information Commissioners Office to discuss.

The Operations Delivery Team will review the completed DPIA and sign off.

Record of Processing Activities (ROPA)

We maintain a register of processing activities of the personal information we are responsible for to ensure it is used according to the data protection principles.

Key points for customers

Keeping customers informed

- When we collect data directly from customers, they have the right to question and be informed of its purpose.
- We will provide details of our data retention, customer rights under the GDPR, how consent can be withdrawn, information on the right to complain and any decision making and profiling that take place using the data.
- We will notify customers if data is transferred to or from a third party.
- Our Data Protection Officer (DPO) is Lee Welsh, and he can be contacted on 0113 386 1000 or lee.welsh@lfha.co.uk.

Access requests

- Customers may make a subject access request (SAR) at any time to find out more about the personal data which we hold, including what we're doing with it and why.
- SARs will normally be responded to within one month however, this can be extended to two months if the SAR is particularly complex or if several requests are made.
- All SARs will be handled by our BI and Data Team and overseen by the DPO.
- We will not charge a fee for handling SARs; however, additional copies or excessive and repetitive requests may result in a charge.

Amending personal data

- Customers have the right to amend personal data that is inaccurate of incomplete.
- We will fix the incorrect data and let them know that it's been completed within one month of the issues being raised and ask any third parties to do the same.

Erasing personal data

- Customers have the right to ask that we erase personal data, but only in the following circumstances:
    - If holding the data no longer serves a valid purpose.
    - They withdraw their consent to us holding and processing the data.
    - The data has been processed unlawfully.
    - The data needs to be erased for us to comply with particular legal obligations.
- We'll comply with all erasure requests, if they are reasonable and lawful, within one month, or two months if the request is complex.

Restrictions of processing personal data:

- Customers can request that we stop processing their personal data and retain only the personal data that is necessary to ensure that further personal data is not processed any further. We will also ask third parties to do the same.

Data portability:

- Data portability allows customers the right to move, copy and transfer their data on request. We will provide all data in PDF format within one month, or two months in complex cases.

Objections to processing personal data:

- Customers have the right to object to us processing their personal data based on legitimate interests, marketing, research, or statistical purposes. In this instance, we will stop processing it immediately.

PECR (Privacy & Electronic Communications Regulations)

- We obtain prior consent for unsolicited marketing by electronic means (calls, texts, emails) unless an exception applies.
- All marketing communications provide a clear opt-out mechanism.
- On our website we inform users transparently about cookies or similar technologies
- We provide a cookie consent mechanism (such as a banner or consent tool) so users can choose / change their preferences.

Key points for colleagues

We will ensure the following measures are taken to make sure all personal data is collected, held, and processed safely and with integrity. We will ensure that:

- All colleagues and anyone working on our behalf are made fully aware of their responsibilities under GDPR and receive annual mandatory GDPR refresher training on Academy. Completion rates will be monitored and picked up with staff if they haven't completed the training.

- Only colleagues and parties working on our behalf will have access to personal data and we will ensure they are appropriately supervised and acting with care and discretion.
- We continually review our collection, storage, and processing methods.

Transferring personal data and communications:

- All emails containing personal data must be sent over a secure network, encrypted and marked 'confidential'.
- If personal data is being transferred in hard copy, it should be passed directly to the individual or sent by registered post and marked 'confidential'.
- We do not transfer data outside the UK

Storing personal data:

- We will store all personal data securely using passwords and data encryption.
- All data will be backed up daily and stored onsite [*is this still the case?*] and offsite.
- All devices will have software to enable them to be wiped remotely.

Use of personal data:

- We will not share personal data without a formal agreement in place and any data transfer should only occur with authorisation from the relevant Head of Service.
- It is the responsibility of the Head of Service to make sure data is provided to third parties only with appropriate consent and that any customers who have 'opted out' are excluded.

Keeping personal data safe:

- All software is designed to require a password, which should be suitably strong and hard to guess.
- Under no circumstances should passwords be written down or shared.
- No software may be installed without the approval of the Head of IT.

Data breaches:

- Any data breaches must be reported immediately to the DPO.
- If a breach is likely to risk the security, rights, and freedoms of any individual, the DPO must inform the Information Commissioner's Office within 72 hours of becoming aware.
- We must inform anyone who has been affected by the data breach.
- Any data breaches or near misses will be investigated by the Data Protection Officer.
- If a breach does occur, we will review our internal processes to learn from any mistakes.

Data Retention

Personal data is kept only for as long as necessary. For example:

- Tenancy records: 6 years after tenancy ends
- Financial records: 6 years
- CCTV footage: 30–90 days (unless required for investigation)
- Complaints: 6 years
- Details of pension fund contributions: Indefinitely

Retention schedules are reviewed annually.

Staff can make also make an SAR relating to their own personal data and can do so using the Request Form and sending it to our Data Protection Officer.

The communication of this policy will be undertaken through Academy, face to face staff training, Team meetings and Quarterly briefings.

Key points for board/committee members and the regulator

Our Board and operations committee are responsible for approving this policy and making sure it supports our objectives to:

- Sustain
- Engage
- Grow

Similarly, our Board, its committees, management, and staff all are responsible for ensuring we remain GDPR compliant.

Policy updates

The BI and Data Team is responsible for updating this policy.

Policy updated and approved 25 March 2026. Next review due 25 March 2028