



IT-POL-03 Data Protection Policy

Version	3	Developed by	Head of Infrastructure & Cyber Security
Approval	07/04/2026	In Consultation With	Assistant Director Systems and Performance
Review Period	3 Years	Document Location	Fred Policies and Information
Classification Type - (Confidential, Restricted, Internal use only, None)			Internal Use Only

Introduction

Framework Housing Association (Framework) processes personal data to deliver housing, care, health, support and employability services, and to meet legal, regulatory and contractual obligations.

This Policy sets out how we will protect personal data and comply with UK data protection and privacy law, including the UK GDPR, Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR), and amendments introduced by the Data (Use and Access) Act 2025 (DUAA).

Purpose

This Policy establishes mandatory controls to:

- safeguard the rights and freedoms of individuals whose data we process.
- ensure lawful, fair and transparent processing aligned to our charitable objects and statutory duties.
- manage risks (confidentiality, integrity and availability) through privacy-by-design/default; and
- demonstrate accountability to regulators, commissioners, service users, residents, staff, volunteers and partners.

Scope

This Policy applies to all Framework staff, Board members, volunteers, agency workers, contractors and third parties processing personal data for or on behalf of Framework, across all systems and media (digital and paper) and all locations. This Policy covers staff, applicants, volunteers, service users/residents, donors, suppliers and all other identifiable individuals. It also applies to joint-controller, controller–processor and controller–controller data sharing arrangements.



IT-POL-03 Data Protection Policy

Data protection principles

FHA complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- it is all accurate and, where necessary, kept up to date and that reasonable steps will 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 ('accuracy')
- it is 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 ('storage limitation')
- it is 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 ('integrity and confidentiality')

FHA will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

Process/procedures/guidance

FHA will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law
- not do anything with personal data that would not be expected given the content of this policy and the fair processing or privacy notice
- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and advising data subjects of their rights
- only collect and process the personal data that it needs for purposes it has identified in advance



IT-POL-03 Data Protection Policy

- ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible
- only retains personal data for as long as it is needed, after which time FHA will securely erase or delete the personal data – FHA's retention schedules (Operations and Central Services) set out the appropriate period of time
- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely

FHA will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, which may lead to dismissal. Obtaining (including accessing) or disclosing personal data in breach of FHA's data protection policies may also be a criminal offence.

Data Subject Rights

FHA has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. Data Protection training is mandatory for all staff, making them aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data has been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

IT-POL-03 Data Protection Policy

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if FHA was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless FHA can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

Special category personal data

This includes the following personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- an individual's health
- a natural person's sex life or sexual orientation
- criminal convictions or offences



IT-POL-03 Data Protection Policy

FHA processes special category data of clients and third parties as is necessary for the provision of health or social care or treatment, in order to provide you with relevant support and/or treatment.

FHA processes special category data of staff as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. FHA also has a data retention policy which sets out how long special category data will be retained.

Roles and Responsibilities

Executive Leadership / CLT: Provide leadership, resources and oversight. Approve policy and monitor assurance.

Policy Owner (Head of Infrastructure & Cyber Security : Maintain policy; oversee compliance; advise on DPIAs; liaise with ICO; maintain ROPA; lead breach/SAR processes; chair or report to the Information Security & Data Protection Forum).

Managers: Ensure team compliance (training, local procedures, retention, access control) and support SARs/breach response.

All Staff/Volunteers: Complete training; follow policy and guidance; report incidents promptly; only access data necessary for duties.

Specialist Functions: HR (staff data), Housing/Support Delivery (service user data), Finance (financial data), SHEQ (H&S), Service Quality (QA), IT (security, systems), Communications (web/cookies).

Compliance, Monitoring and review

Compliance will be monitored via the Information Security & Data Protection Forum, internal audits, incident and SAR metrics, and management reporting.

Policy effectiveness will be reviewed at least every three years, or sooner on material legal/regulatory change (e.g., further DUAA commencement, ICO guidance updates).

Non-compliance may result in disciplinary action and/or regulatory reporting.