Data Protection Policy

1. Aim and scope of policy

This policy sets out our approach to the UK General Data Protection Regulation (UK GDPR), Data Protection Act (DPA) 2018 and any other applicable data protection legislation. It applies to all personal data we hold relating to any identifiable living person.

We're a data controller and a data processor. We maintain our appropriate registration with the Information Commissioners Office (ICO) as per our data controller responsibilities as we process personal data. Our registration number is ZA248321.

2. Definitions

Personal data

Data which can identify an individual - for example name, home address, IP address, tenancy reference number, email address and phone number.

Special category data

Data which includes information about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, criminal offences and genetic or biometric information.

3. Policy

3.1 Principles

We're committed to complying with all data protection legislation and following best practice in the protection of the rights and freedoms of data subjects whose information we collect and process.

3.1.1 Lawful, fair and transparent

We process personal data and special category personal data fairly, lawfully and in a transparent manner.

We apply at least one of the following lawful basis (conditions) when handling personal data:

- Consent - we hold recent, clear, explicit, and defined consent from an individual to process their data for a specific purpose.
- Contract – we process data to fulfil or prepare a contract for the individual.
- Legal obligation - we have a legal obligation to process the data.
- Vital interests – we process the data to protect human life.
- Public interest– we process the data to carry out a task of public interest.
- Legitimate interest – we process data for our legitimate interests e.g. carrying out surveys to help us to improve our services in the interests of our customers.

In addition, for special category data, we also apply at least one of the following conditions:

- Explicit consent
- Employment law, social security and social protection law
- Vital interests

- Carried out by foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim
- Data made public by the data subject
- Establishment, exercise or defence of legal claims
- Substantial public interest
- Purposes of preventative or occupational medicine
- Public interest (public health)
- Public interest (archiving, scientific or historical research or statistical purposes)

We maintain an Information Asset Register (IAR) which outlines our processing activities. It states what data we hold, where we hold it, why we hold it, who we share it with and how long we retain it for. We keep this register up to date and relevant.

3.1.2 Limited for its purpose
We only collect data for specific purposes. Our privacy notice is available on our website and our intranet (VIV), it details what data we process, why and in what circumstances it's shared.

3.1.3 Data minimisation
We collect necessary data which is not excessive for its purpose.

3.1.4 Accurate
We rely on individuals to provide us with accurate data and to tell us if their personal data needs updating.
We regularly check that contact details are up to date and accurate when we're in contact with our customers.

3.1.5 Retention
It's important that we only collect information which is not excessive for its purpose and ensure that we only keep it for the length of time that we need it. We keep information in line with the NHF retention schedule unless it has been agreed otherwise.

We'll have some information that we must keep for a legal purpose, to help our business run and to ensure that our information is easily accessible. However, not all information needs to be or should be kept indefinitely. Keeping information indefinitely could expose us to risk as well as having a storage and cost impact.

We've set retention periods with all areas of the business, across our systems. We should stick to the retention periods we have set unless there is a justified reason for us to change them, any changes should be reviewed and agreed with the Governance team and the Head of Service for the area.

3.1.6 Integrity and confidentiality
We keep personal data secure against loss or misuse by following our Information Systems Security and Acceptable Use Policy.

Any personal data protection incidents are managed in accordance with our Data Protection Incident Procedure.
Our data processing agreement reflects where third parties process personal data on our behalf.

3.2 Rights of individuals
Individuals have rights in relation to their data which we respect and comply with as per our regulatory obligations.

3.2.1 Right to be informed
We provide concise, transparent, intelligible, and easily accessible privacy notices free of charge.

We keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

3.2.2 Right of access
We facilitate individuals' access to their personal data upon an access request.

3.2.3 Right to rectification
We'll correct an individual's personal data if it is inaccurate or incomplete.

3.2.4 Right to erasure
We'll erase personal data and cease processing, upon request, unless we have a lawful basis to continue processing.

If personal data has been processed by third parties, we will inform them of their obligations to erase the data.

3.2.5 Right to restrict processing
We'll restrict, block, or suppress the processing of personal data upon request, unless we have a lawful basis to continue processing.

3.2.6 Right to data portability
We'll provide personal data to an individual upon request, so that it can be reused for their purposes, free of charge and in a commonly used, machine-readable format.

3.2.7 Right to object
We'll respect an individual's right to object to certain processing for example, marketing to individuals. We'll explain if there are circumstances which mean we are unable to do this.

3.2.8 Rights in relation to automated decision making and profiling
We'll offer simple ways to request human intervention or challenge any automated decision.

3.3 Third parties
We've contracts in place with third parties who handle your data. This will detail both ours and their liabilities, obligations, and responsibilities. We only appoint processors who can provide sufficient guarantees of compliance with data protection legislation.

If we act as a data processor for a data controller, we'll act on the instructions of the controller and acknowledge our responsibilities as a data processor.

3.4 Reporting Data Protection Incidents

In line with our Data Protection Incident procedure, any data protection incident must be reported immediately to the Governance team and the individual's line manager. We'll report any high-risk data breaches to the Information Commissioner's Office within 72 hours.

3.5 Data Protection Impact Assessments

We're required to undertake an impact assessment on projects, new technologies or changes in the way in which we process personal data. An impact assessment helps us to identify and appropriately address any privacy risks or concerns when processing an individual's information.

3.6 Closed Circuit Television (CCTV)

We've several CCTV cameras located within our properties and our offices. The purpose of these cameras are to detect, prevent and reduce the incidence of crime, to investigate anti-social behaviour cases, protect our properties and assets and for the safety of our staff. We manage the camera equipment, images, and footage to ensure that we are compliant with data protection laws.

3.7 Complaints

Any data protection complaints received will be handled in line with our complaints policy. This does not affect your right to complain to the Information Commissioner's Office.

4. Responsibilities

All staff must:

- fully understand and comply with this policy
- complete data protection online training annually

The Data Protection Officer has:

- overall responsibility for the day-to-day implementation of this policy
- responsibility for arranging data protection training and providing professional advice as required
- responsibility for liaising directly with the ICO

Executive team:

- will review and approve this policy on an annual basis

5. Related documents

- Privacy Notice (available on our website and VIV)
- Data Protection Impact Assessment
- Data Protection Incident Procedure
- Information Systems Security and Acceptable Use Policy
- Transparency Policy
- CCTV Procedure
- Complaints policy

Author	Owner	Approval level e.g. Board	Date approved	Review date
Data Protection Officer	Data Governance Lead	The Executive Team	May 2024	May 2025