WestKent
Places to live. Space to grow.

Places to live. Space to grow.

Data Protection and Retention Policy

Policy Author: **Data Protection & Policy Officer**

Policy Owner: **Head of Risk and Governance**

Effective date: August 2024

Next review date: **July 2026**

Version Control:

Issued Date	Approved by	Version
01-Aug-2024	Audit & Risk Committee	1

CONTENTS PAGE

1 Introduction and Purpose

1.1 This policy sets out the ways in which we will process and store the personal data of individuals. West Kent is a data controller as defined under data protection legislation. We need to collect, use, store, share and delete certain types of information about people we deal with to operate as a housing association and a registered charity.

1.2 The United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations (PECR) are the main pieces of data protection legislation in the UK, in addition to various codes of practice, guidelines and case law. All staff must comply with data protection legislation. Failure to comply can result in enforcement action from the Information Commissioner's Office (the ICO), and also criminal investigations against individuals.

1.3 The UK GDPR definition of personal data includes any information relating to an identified or identifiable natural living person. This includes data which doesn't explicitly reference an individual, but where the identity of the individual can be deduced.

2 Responsibilities

2.1 Board

The Audit & Risk Committee is responsible for the overview and scrutiny of data protection compliance.

2.2 Data Protection Officer

The Data Protection Officer is responsible for ensuring that an appropriate framework is in place for compliance with data protection legislation; overseeing Subject Access Requests and breach investigations; the submission of appropriate reports on compliance to management and the Information Commissioner's Office, undertaking regular reviews of compliance and making recommendations to improve compliance.

2.3 Head of Governance and Risk

The Head of Governance and Risk is responsible for monitoring and reporting compliance with data protection legislation to the Executive Team and Audit and Risk Committee.

2.4 Information Resilience Working Group

The Information Resilience Working Group monitors compliance with the accountability framework, measures progress with the data protection action plan, manages data protection risks, reports on information security and infrastructure risks, as well as compliance across all West Kent systems and processes.

2.5 All employees

All employees are responsible for complying with data protection legislation, this policy and all other guidance and training provided by West Kent. All employees must report any data protection

issues (including data breaches) they come across to their manager and the Data Protection Officer at dataprotection@wkha.org.uk.

3 Legislation and Regulation

3.1 The Data Protection Act (DPA) 2018 came into force on 25 May 2018 and was designed to implement the EU Data Protection Directive (EC/95/46). The Act updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), and extending data protection laws to areas which are not covered by the GDPR or the Law Enforcement Directive.

3.2 Since then, subordinate legislation has come into force and this process is expected to continue. The main objective of the DPA is to provide a framework in which the rights and freedoms of individuals can be protected. It also attempts to strike a balance between that requirement and the needs of organisations to use information for the purposes of their business.

3.3 Article 5 GDPR in particular sets out seven key principles related to the processing of personal data, which data controllers to be aware of and comply with when collecting and otherwise processing personal data:

1. Lawfulness, fairness and transparency - all data must be collected and processed lawfully, fairly, and transparently.
2. Purpose limitation – all data must only be collected for specified, explicit, and legitimate purposes that have been made clear to data subjects at the start of the processing.
3. Data minimisation – all personal data processed must be “adequate, relevant and limited”
4. Accuracy - reasonable efforts should be made to ensure that collected personal data is accurate and kept up to date.
5. Storage limitation - personal data must not be held for any longer than is necessary for fulfilling the stated purposes.
6. Integrity and confidentiality - measures to secure the integrity and confidentiality of the data you collect and process must be taken.

4 Policy Statement

4.1 The Association needs to collect, manage, and use personal data about its present, former, and potential residents and stakeholders in order to uphold the tenancy agreement and meet our legal and regulatory obligations to sector bodies and government.

4.2 The Data Protection Policy sets out how personal data will be managed by the Association, and its responsibilities in ensuring it complies fully with the provisions of the UK GDPR and the Data Protection Act (DPA) 2018. To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

4.3 All West Kent Housing Association staff have a responsibility to protect personal identifiable data and respect the data protection rights of all data subjects, in accordance with the 7 principles of the UK GDPR. This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarise themselves with and act in accordance with this policy.

4.4 The Association may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with the Association’s

policy framework. Any failure to follow this policy by staff or stakeholders may result in disciplinary action.

5 Reporting

5.1 We maintain a policy of logging all data rights requests, and investigating data breach complaints, incidents and near misses. All incidents and data breaches will be reported on a quarterly basis to the Executive Team and the Audit & Risk Committee by way of a data protection compliance report.

5.2 The Data Protection Act 2018 requires that we must report reportable data breaches to the ICO within 72 hours. Further guidance on the process for data breaches can be found in Data Breach Procedure, which is located on our internal intranet, Bettie.

6 Consultation

6.1 The Resident Impact Assessment (RIA) was conducted to assess how the policy may impact residents. The RIA concludes that there is low risk of negative impact on residents and therefore residents will not be directly consulted regarding this policy. Any changes that will affect residents, will be communicated in our privacy notices on the West Kent website.

6.2 The Equality Impact Assessment was conducted to ensure that our policies, practices, events and decision-making processes are fair and do not present barriers to participation or disadvantage any protected groups from participation. This policy is compliant with the Equality and Diversity Policy.

7 Communication

7.1 The data protection and retention policy will be published via our internal intranet, Bettie and will be available to the public upon request.

7.2 We will publish Privacy Notices which inform data subjects how we collect and store their personal information. The Privacy Notice will state the lawful basis for processing and who we'll share data with. If we make any changes to our notice, we will publish the changes on our website without undue delay.

8 Principles

8.1 There are seven principles of data protection as detailed in the Data Protection Act 2018 which encompass everything we need to do as a business to comply.

8.2 <u>Lawful, fair and transparent processing</u>
We will only process personal data in a lawful, fair and transparent manner. We will maintain a record of all activities across West Kent which use personal data. We will ensure that we have a lawful basis for each of our data processing activities.

We will publish privacy notices on our website which explain:

- What data we collect
- The reason we collect the data
- How we will use the data
- Who we share it with
- How long we will keep the information

8.3 Purpose limitation

We will only use personal data for the purpose it was originally collected for. The exception to this is where a new purpose is compatible with the original purpose and has been assigned a lawful basis. In this case we will inform the individual of the new purpose of processing their data.

8.4 Data minimisation

We will only process the personal data that is necessary to carry out the processing required.

8.5 Accuracy

We will ensure that the personal data we hold is as accurate as possible.

8.6 Storage limitation

We will only keep personal data that we need to carry out the processing required. Personal data will be deleted in line with our retention schedule (Appendix one).

8.7 Integrity and confidentiality

We will employ appropriate technical and organisational measures to ensure the personal data we process is protected from unauthorised or unlawful processing and against accidental loss, destruction or damage. We will maintain a list of all data processors we employ. We will enter into legally enforceable data sharing agreements with our data processors and conduct due diligence to ensure they meet security requirements.

8.8 Accountability

We will employ a Data Protection Officer to monitor compliance with data protection legislation and raise compliance issues. We will conduct audits to check we comply with the data protection legislation principles and report this to Board.

8.9 Rights under the Data Protection Act 2018

Individuals have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making.

8.10 We will comply with any request by an individual to exercise their rights within the required statutory deadlines of the request being made. If you would like to exercise any of your rights above please contact our Data Protection Officer at dataprotection@wkha.org.uk. Please see Appendix 3 for the Association's full SAR Procedure.

8.11 Freedom of Information Act 2000 does not currently apply to Housing Groups. However, the Association has adopted the principle of being as open as possible in its business, and restricting the withholding of information solely to that of commercially sensitive information.

9 Lawful bases for processing personal data

9.1 The UK GDPR only allows processing for 6 lawful bases, namely:

a) data subject has given consent;
b) the processing is necessary for the performance of a contract
c) to meet our legal compliance obligations;
d) to protect the data subject's vital interests;
e) for the performance of a task carried out in the public interest or in the exercise of official authority;
f) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

9.2 If you are relying upon (f) 'legitimate interests' as the legal basis for processing, you may need to complete a Legitimate Interest Assessment (LIA) using the LIA Template (appendix 4).

10 Special category data

The legal bases set out above do not apply to the following categories of personal data which are referred to as "special categories of personal data": Some personal data is more sensitive and is afforded more protection. This is information related to:

- Ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life and/or sexual orientation
- Criminal data (convictions and offences)

10.1 If we are processing a special category of personal data we must also have one of the following legal bases for the processing;

a) explicit consent from the data subject;
b) for the purposes of carrying out obligations or rights in the field of employment and social security and social protection law providing for appropriate safeguards for the fundamental rights and interests of the data subject;
c) to protect the data subject's vital interests;
d) to pursue legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members of the body or persons with regular contact and the data is not disclosed outside that body;
e) the personal data is manifestly made public by the data subject;

f) it is necessary for legal claims;
g) it is necessary for substantial public interest and measures to safeguard the rights of the data subject are provided;
h) it is necessary for preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems and services;
i) necessary for public interest in public health such as protecting against serious cross border threats to health;
j) it is necessary for archiving in the public interest, scientific or historical research purposes or statistical purposes.

11 Training and employees

11.1 All employees:

(a) Must undertake mandatory data protection training when they join West Kent and complete annual refresher training.
(b) Must assess and manage the risks around how they process personal data using DPIAs
(c) Must collaborate with the DPO to maintain the associations' records containing personal data in compliance with the Record of Processing Activities (ROPA) and the Information Asset Register.

11.2 We will provide targeted data protection training to teams and individuals when a need is identified.

11.3 Training compliance is monitored and reported to the Executive Team and Audit and Risk Committee on a quarterly basis.

11.4 The Association will take appropriate disciplinary action against employees, officers, trainees, members, Association representatives or suppliers found breaching the Policy where appropriate to them.

12 Data protection by design and default

12.1 We will consider data protection and privacy from the outset for any new project, service or system. We will do this by conducting Data Protection Impact Assessments (DPIAs) and seeking advice from the Data Protection Officer.

12.2 We will carry out DPIAs where there is a high risk to the rights and freedoms of individuals or we are using new technology. We will also carry out DPIAs where we are using personal data in a new or different way. We will carry out all DPIAs in consultation with the Data Protection Officer.

13 Data breaches

13.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

13.2 When a data breach occurs, we will assess the likelihood and severity of the resulting risk to individuals' rights and freedoms. These assessments will be carried out by the Data Protection Officer and relevant staff members.

13.3 If it is likely that there is a risk to the rights and freedoms of individuals, we will inform the Information Commissioner's Office. If it is likely that there is a high risk, we will inform these individuals directly as soon as possible.

13.4 Please see Appendix 2 for the Association's full Data Breach Procedure.

14 West Kent as a data processor

14.1 For some data processing activities, we are considered a data processor under data protection legislation. In these circumstances, we will follow the instructions of the data controller and our obligations under data protection legislation that apply to data processors.

15 Retention and Disposal of Data

15.1 The Association discourages the retention of Personal Data for longer than it is necessary. Some Personal Data will be kept for longer periods than others. Considerable amounts of data are collected about residents and employees, however the length of retention depends partly on generally accepted best practice and partly on legal requirements.

15.2 Periods of retention will be considered using the periods set down in the Limitation Act 1980 after which legal proceedings are time-barred (generally between 3 and 12 years depending on the type of claim.

15.3 Documents should be retained for an appropriate period and should then be destroyed or discarded within a reasonable period after the end of the retention period. The minimum recommended time for the retention of are documents are listed in Appendix 1. The retention times shown are mainly based on advice issued by The National Housing Federation and independent legal advice obtained by the Association when developing this policy.

15.4 The Group staff should consider the following questions when deciding how long to retain a record before final disposition:

- Are the documents still required for the day-to-day running of the Association?
- Is it required for legal purposes (e.g. contracts)?
- Does any legislation or official regulation govern how long it must be kept?
- Is it likely to be of ongoing or recurrent public interest?

15.5 The retention schedule and policy should be maintained and implemented by the Data Protection Officer, and any changes to the schedules should be approved by the Head of Risk and Governance, and the change (if agreed) should be reflected without undue delay.

16 Disposal Procedures

16.1 It is essential that the disposal of records is undertaken in accordance with these policies and procedures.

16.2 All paper-based records containing personal information should be shredded or disposed of through confidential waste bins located around the offices.

16.3 All electronic records containing personal information should be deleted completely from the hard drive.

16.4 All information contained within our housing system will be cleansed through our Archive Module with on a regular basis.

16.5 Records which are not selected for permanent preservation and which have reached the end of their administrative shelf life should be destroyed in as secure a manner as is necessary for the level of confidentiality or security markings they bear.

17 Review and Updates

17.1 We will review this policy on a 3 yearly basis or when there are changes to the Data Protection Act 2018.

APPENDIX 1 – Retention Schedule

Our full retention schedule is available on Bettie or at our offices.

Document	Retention Period	Retention Trigger
Accident books and records and reports of accidents	6 years after date of occurrence/entry	Date of occurrence
Applications for accommodation	6 years after offer accepted	Offer accepted
Application forms, interview notes	6 years after offer accepted	Offer accepted
ASB case files	5 years or until end of legal action	
Board meetings/residents' meetings	10 years from the date of the meeting of extant company or life of company	Date of meeting
Board Members Documents	6 years after board membership ceases though some details should be destroyed when membership ceases e.g. bank details.	Membership ceases
Documents proving the right to work in the UK	Duration of employment	End of employment
Documents relation to successful tenders	6 years	End of contract
Documents relating to unsuccessful form of tender	2 years after notification	After notification
Facts relating to redundancies	6 years	Date of redundancy
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently	Permanently
Health records	6 years from date of sickness	6 years from date of sickness
Housing Benefits Notifications/Universal Credit Notifications	2 Years	
Income tax, NI returns, correspondence with tax office	6 years	End of Financial Year
Lease documents	15 years after expiry	Lease expiry
Membership records	6 years	Membership ceases
Payroll	3 years	End of Financial Year
Personal files including training records and notes of disciplinary and grievance hearings	6 years	End of employment
Pensioners records	12 years after benefits cease	After benefits cease
Records relating to working time	6 years	End of employment
Records relating to offenders. Ex-offenders (sex	While tenancy continues	While tenancy continues

offender register)		
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years	Date of redundancy
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years	After transfer or value taken
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	6 years	On payment
Statutory Sick Pay records, calculations, certificates, self-certificates	6 years from date of sickness	Date of occurrence
Tenancy files	6 years after offer accepted	Offer accepted
Care plans/ case files for adults and related documents	8 years from end of care. (Adult Social Care)	End of support
Wages/salary records, expenses, bonuses	3 years	End of Financial Year

APPENDIX 2 – Data Breach Procedure 2023

18 Introduction

18.1 West Kent Housing Association (WKHA) collects, holds, processes and shares large amounts of personal data and has an obligation to ensure that it is kept secure and appropriately protected.

18.2 This document details the procedure that must be followed to ensure a consistent and effective approach in managing personal data security breaches.

19 Purpose

19.1 The purpose of this procedure is to ensure that:

- personal data breaches are detected, reported, categorised and monitored consistently
- incidents are assessed and responded to appropriately without undue delay
- decisive action is taken to reduce the impact of a breach
- improvements are implemented and communicated to prevent recurrence or future incidents
- certain personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours, where required.

20 Scope

20.1 This procedure applies to all staff, partner organisations and partner staff, suppliers, contractors, consultants, representatives and agents that work for or process, access, use or manage personal data on behalf of WKHA.

20.2 This procedure relates to all personal and special category ('sensitive') information handled, stored, processed or shared by the University whether organised and stored in physical or IT based record systems.

21 Definitions

21.1 A **"Data Breach"** incident includes but is not limited to:

- **"Alteration of personal data"** – refers to manipulating or changing information, as well as deleting partial information, without permission
- **"Destruction of personal data"** refers to the process of making personal data inaccessible, non-retrievable and re-useable by any person in any way where there is a legal requirement to keep the

data. This also may be physical destruction which may include shredding, pulping or burning paper records.

- **"Loss/theft of personal data"** refers to loss or theft of laptop, iPad/tablet device, mobile device or paper records. This can occur due to human error, viruses, malware, or power failure. It may also occur due to physical damage or mechanical failure.
- **"Special category data"** is personal data that needs more protection because it is sensitive. It can include revealing racial or ethnic origin. Political opinions. Religious or philosophical beliefs. Trade union membership.
- **"Unauthorised access to personal data"** refers to access to, or modification of, data or information systems. As well as attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- **"Unauthorised disclosure of personal data"** – refers to the disclosure or release of protected information which is not in accordance with West Kent policies. This could be as a result of deception, social engineering, phishing and blagging. This can also occur following a website defacement, hacking attack, sharing personal data without a data sharing agreement or processing data by a processor without a legally binding contract in place. Unforeseen circumstances such as a fire or flood; leading to unavailability of systems processing personal data, is also included.
- **"Personal data"** is information that relates to an identified or identifiable living individual.
- **"Personal data breach"** means 'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. Some other examples include:
  - Sending personal data to an incorrect recipient
  - Data input error / human error
  - Non-secure disposal of hardware or paperwork containing personal data
  - 'Blagging' offences where information is obtained by deceiving the organisation who holds it

22 Reporting the Breach

22.1 The following steps should be followed by the colleague who discovers that a potential data breach may have occurred.

22.2 You must contact the Data Protection Team as soon as you become aware a data breach has occurred, or you suspect a breach may have happened.

22.3 West Kent is legally required to assess and report serious data breaches to the regulator (the Information Commissioner's Office) within 72 hours, so it is particularly important that the Data Protection Team is able to commence investigation as early as possible.

22.4 Either call a member of the team on 01732 749400 or email dataprotection@wkha.org.uk. If you call the team, please ensure that you confirm the details reported in writing via email. The Data Protection Team should follow up in writing to confirm receipt, without undue delay.

22.5 Once the risk is assessed, the data protection team will open an investigation. A breach incident report will be completed by the parties involved and the data protection officer will produce a report, with a conclusion of any further action. The investigation report will be signed off by the Head of Risk and Governance, Executive Team or Chief Executive depending on the scale and severity of the incident.

22.6 Any reportable breaches will be sent to the Board for review.

22.7 The Data Protection Officer will record all breaches (reportable or non-reportable) on our internal breach log.

23 Containing the Breach

23.1 The following steps should be followed by the Data Protection Officer in the Data Protection Team, once a data breach has been established.

23.2 Depending on the type of breach, action must be taken to stop the breach from happening further.

23.3 Examples of this type of action could be changing passwords, isolating parts of the network, taking down web pages, restricting access to systems, or restricting access to the offices.

24 Recovering the Data

24.1 Depending the type of breach, action must be taken to attempt to recover data where possible.

24.2 Examples of this type of action could be physical recovery of the data or equipment, using backups to recover corrupted data, recalling emails (or asking recipient to delete the email if recall is not possible) or retrieving paper documents.

25 Establishing the Size and Scope of the Data Breach

25.1 The size and scope of the breach needs to be established. This involves asking questions such as:

The size and scope of the breach needs to be established. This involves asking questions such as:

- How many individuals have been affected by the breach?
- What type of data has been breached?
- What has happened to the data?
- Whose data has been breached?
- What safeguards are in place to protect the data such as encryption or password protection?

26 Assessment of Risk

26.1 The risk to the individuals needs to be assessed. Harm to the individual can take many forms such as identity theft or fraud, financial loss, discrimination, damage to reputation, physical harm or emotional distress.

26.2 Assessing the risk to the individual involves asking questions such as:

- How sensitive is the data?
- What could the data tell a third party about the individual?
- What harm can come to those individuals?
- Are there organisational consequences we should consider such as reputational risk?
- Are there any other steps we can take to help mitigate harm to individuals such as contacting relevant banks if financial data has been breached?

27 Notification

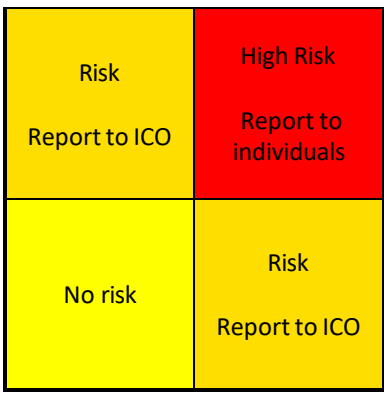
27.1 Not all data breaches need to be notified to the Information Commissioner's Office (ICO) or relevant individuals.

27.2 Breaches which pose a risk to the rights and freedoms of individuals must be reported to the ICO within 72 hours of becoming aware of the breach. If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

27.3 Breaches which pose a high risk to the rights and freedoms of individuals must also be reported to the individuals without undue delay.

27.4 Criminal breaches: If the security incident or personal data breach is thought to be a criminal act or involve a criminal act (such as theft of equipment or data), the Data Protection Officer should inform the police.

27.5 The Data Protection team should also check whether they have any contractual obligations to notify partners of the breach. (e.g. if it related to an information sharing initiative with a local authority).



28 Learning

28.1 Depending on the outcome of the breach investigation, learning should be identified and shared with relevant stakeholders.

28.2 The Data Protection Team may provide additional training where required by role or in the event of an incident taking place to help employees identify a breach and understand the impacts breaches can cause.

Summary of Key Material

- **New Retention Policy**
  A new retention policy has now been incorporated into the Data Protection Policy, and this encompasses all processes and guidelines that West Kent should follow to ensure compliance with data storing, retention and archiving.

- **New Retention Schedule**
  The new retention schedule list the types of record or information we hold, what we use it for, and how long we intend to keep it. The schedule will establish and document standard retention periods for different categories of personal data. Once the retention time period for a particular data set expires, it can be deleted or moved as historical data to an archived storage, depending on the requirements.

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS

Legislation	Data Protection Act 2018 General Data Protection Regulations
Related Policies	Data Breach Procedure 2023 Data Processing Procedure 2022 Subject Access Request Procedure 2024
Appendix	Appendix 1 - Retention Schedule
Forms	Equality Impact Assessment Resident Impact Assessment Legitimate Interests Assessment