DATA PROTECTION POLICY

Classification: Management

Status: Approved

Policy Lead:	Director of Business Support
Date Approved:	April 2025
Review Due Date:	April 2028
Review Period:	3 years unless required earlier due to changes in the law, regulation, best practice or requirement of the Association

REFERENCE PAGE

Document Title:	Data Protection Policy (previously Privacy Policy)
Aim:	Good information governance and data protection compliance are an integral part of our work. We hold a wide range of personal information and special categories of information. We have a duty to protect this information and ensure it is not seen or accessed by people (whether internal or external) without the authority to do so.
Objective:	1 Governance: Ensure we continue to have strong leadership in the Association
Scope of Policy:	All employees (whether permanent or temporary) including those that are mobile working and working off site or working within joint partnerships, agency works, contractors, consultants, modern apprentices, secondees and work experience placements shall comply with this Policy and must be aware of what they must do to protect the security of information processed.
Nominated Officer:	Data Protection & Information Officer
Approval Source:	Executive Team – Minor changes otherwise Board
Legal and Regulatory References:	The relevant legislation in relation to theprocessing of data is : • Data Protection Act 2018 • UK General Data Protection Regulation derived from the EU's General Data Protection Regulation (GDPR). • The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amendedby the proposed Regulation on Privacy and Electronic Communications);
Procedural References:	• Privacy Notices • Information Security Awareness Procedure • Information Disposal and Retention Policy • Data Sharing Register Procedure • Data Protection Impact Assessment Procedure, Guidance & Template • Legitimate Interests Assessment Guidance • Legitimate Interests Assessment Template • DPIA Procedure • DPIA Template
Consultation Completed:	N/A
Risk Implications:	1. Existing Policy, minimal change Policy sets out the framework to manage the risks associated with the holding of personal data relating to our customers, colleagues and other data subjects
Equalities Assessment:	Required
Accessibility:	Accessible electronically/online and in print. All documents can be translated and made available in audio, braille and large print versions upon request.
Publish on Website:	Yes

CONTENTS

1. INTRODUCTION

This policy sets out how Eildon Housing Association (hereinafter “Eildon”) will ensure that personal data held relating to our customers, colleagues and other data subjects is processed in line with the seven key data protection principles of:

a) Lawfulness, fairness and transparency: data is processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Purpose limitation: data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) Data Minimisation: data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accuracy: data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purpose for which it is being processed. If no longer required, it should be erased without delay;

e) Storage Limitation: data 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 is processed.

f) Integrity and Confidentiality (security): data 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.

g) Accountability: data protection measures are documented and sufficient.

These statements set out Eildon’s main responsibilities under the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) which is derived from the EU’s General Data Protection Regulation (GDPR).

This policy defines the framework for management of personal data and Eildon’s duties in the processing of that data.

2. DATA SCOPE

Eildon holds a variety of data relating to individuals, including customers, colleagues, and other individuals (also referred to as Data Subjects). Data which can identify Data Subjects is known as Personal Data.

- 'Personal Data' is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by Eildon
- Eildon also holds Personal Data that is sensitive in nature (i.e., relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is 'Special Category Personal Data' or 'Sensitive Personal Data'.

This policy applies to all personal data recorded and processed by the Eildon Group and its subsidiaries.

3. PROCESSING OF PERSONAL DATA

Our Privacy Notices and the addendum of terms and conditions of employment provided provides visibility and transparency about the personal data we collect and process. They outline the legitimate grounds for processing together with what we will and won't do with personal data.

Eildon is permitted to process personal data on behalf of Data Subjects provided it is doing so with a valid lawful basis:

- **Consent**: the individual has given clear consent for us to process their personal information for a specific purpose.
- **Contract:** processing is necessary for the performance of a contract between Eildon and the Data Subject or for entering into a contract with the Data Subject.
- **Legal Obligation**: is necessary for Eildon's compliance with a legal obligation.
- **Vital Interests:** is necessary to protect the vital interests of the Data Subject or another person.
- **Public Task:** the processing is necessary for Eildon to perform a task in the public interest or for official functions, and the task or function has a clear basis in law

In the event of Eildon processing Special Category Personal Data or Sensitive Personal Data, Eildon must rely on an additional ground for processing in accordance with one of the special category grounds. These include but are not limited to:

- The Data Subject has given explicit consent to the processing of this data for a specifiedpurpose.
- Processing is necessary for carrying out obligations or exercising rights related to employment, social security, or social protection law.
- Processing is necessary for health or social care.
- Processing is necessary to protect the vital interest of the Data Subject or, if the Data Subject is incapable of giving consent, the vital interests of another person.
- Processing is necessary for the establishment, exercise, or defence of legal claims, or whenever a court is acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest under law.

We will generally avoid relying on consent because of the imbalance of power between Eildon and our customers and colleagues. Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4. PRIVACY NOTICES

Privacy Notices will be issued to all Data Subjects at the onset of processing personal data. Our Privacy Notices are available on our website at: https://www.eildon.org.uk/library/#115-privacy and any linked online service websites. We will review our Privacy Notices regularly, but at least annually, to ensure that they are accurate and up to date. Any revisions will be reviewed and agreed by the Executive Team.

5. DATA MANAGEMENT

Our approach to data management ensures that we consider how data, when collected, is held securely throughout its lifecycle, supporting the general obligation under UK GDPR of data protection by design and default..

We will do this through:

Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment is designed to analyse, identify and minimise data protection risks. This helps us assess and demonstrate compliance with our data protection obligations.

Conducting a DPIA is a legal requirement for any type of processing that is likely to result in a ‘high risk’ to the rights and freedoms of individuals. The ICO has published a list of the kind of processing operations that are likely to be high risk and will require a DPIA.

Use of new or innovative technologies. Processing involving the use of new technologies, or the novel application of existing technologies (including AI).
Denial of Service. Decisions about an individual's access to a service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
Large scale profiling. Any profiling of individuals on a large scale.
Biometrics. Any processing of biometric data.
Genetic Data. Any processing of genetic data.
Data matching. Combining, comparing or matching personal data obtained from multiple sources.
Invisible processing. Processing of personal data that has not been obtained direct from the data subject.
Tracking. Processing which involves tracking an individual's geolocation or behaviour, including in the online environment.
Targeting of children or other vulnerable individuals. The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making
Risk of physical harm. Where the processing is such that a personal data breach could jeopardise the physical health & safety of individuals**.**

Eildon will ensure that a DPIA is undertaken before we embark on any new project, policy or process which involves large scale processing, new processing or monitoring, decides on access to services or opportunities or involves sensitive or special category data.

The outcome of a DPIA will be reviewed by the Data Protection and Information Officer and authorised by a relevant Director and any action outcomes integrated into project and implementation plans.
.

In the event that Eildon are unable to reduce or mitigate risks identified within a DPIA, Eildon are required to consult with the Information Commissioners Office.

A Data Protection Impact Assessment template, procedure and guidance is available here for managers undertaking DPIA's

Legitimate Interests assessment (LIA)

In all other instances Eildon will use a Legitimate Interests assessment to ensure any new or existing processing is lawful. An LIA is a type of light touch risk assessment on a specific context or circumstance. Recording our reasoning in a LIA will also help us demonstrate compliance with our accountability obligations under GDPR.

The outcome of a LIA will be reviewed by the Data Protection and Information Officer and authorised by a relevant Director.

A Legitimate Interests template and guidance is available here.

Data Minimisation

Ensuring that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Data Accuracy

Taking reasonable steps to ensure personal data is accurate and where necessary for the lawful basis on which data is processed, steps are put in place to ensure that personal data is kept up to date i.e., it is changed when a customer notifies us of a change, and we proactively look to refresh critical core data.

Data Sharing

Where we need to share data with third parties for the purpose of delivering day to day services, we may require the third-party organisations to enter into a Data Sharing agreement or Addendum with us governing the processing of data, security measures to be implemented and responsibility for breaches. The type of agreement required will depend on the relationship with the third party i.e., Data Controller – Data Processor, Data Controller – Joint Data Controller. We will keep a record of these agreements as part of our Data Sharing Register.

Data Retention and Deletion

Eildon will ensure that personal data is kept for no longer than necessary. We will put in place an Information Disposal and Retention policy which details the retention periods for each functional area in which data is processed and review this annually. This schedule will reflect what data should be retained, for how long and why.

Management of document retention and disposition will largely be managed in our Microsoft 365 SharePoint environment.

Data Storage and Security

We will ensure that personal data is stored securely in paper form or using modern software that is kept-up-to-date. Access to personal data will be limited to colleagues who need access and appropriate security will be in place to avoid unauthorised sharing of information. When sharing data with third parties we will ensure that data is encrypted, or password protected. When personal data is destroyed this will be done safely such that the data is irrecoverable. In all cases appropriate back-up and disaster recovery solutions shall be in place.

We will publish a Data Retention Schedule which will be reviewed on an annual basis by the Data Protection and Information Officer with input from the Leadership Team and other key officers within Eildon. The Executive Team will consider the outcome of this review and where required approve the amendments required.

6. RESPONSIBILITY

Eildon is responsible for; and must be able to demonstrate compliance with responsibilities under UK data protection law.

The Board has delegated overall responsibility for this policy to the Executive Team. The Code of Conduct signed by members of Eildon's Board includes an acknowledgement of an absolute duty of confidentiality to Eildon. This states that Board members must not disclose to any third party any confidential information which they have obtained because of their position on the board

The Audit & Risk Committee will obtain assurances relating to the adequacy and effectiveness of risk, control and governance processes relating to data protection and privacy in Eildon. The committee will do this by instigating and receiving reports on Eildon's compliance with the principles of this policy data protection law.

Leaders are responsible for ensuring that all colleagues in their teams understand the Data Protection Policy and principles and the underlying UK data protection law. Leaders must also encourage the reporting of data protection incidents as part of a commitment to continuously improving standards of data protection and privacy.

All colleagues are required, by the Code of Conduct for Staff Members to abide by procedures designed to protect the confidentiality of information held about customers, other colleagues or others. Data Protection training is provided as mandatory during induction and refreshed annual thereafter.

Eildon has appointed a Data Protection & Information Officer (DPIO). The DPIO's details are noted on our website and contained within our Privacy Notices.

The Data Protection & Information Officer is responsible for the following tasks:

- To inform and advise Eildon and colleagues about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; train colleagues and conduct compliance audits; and
- To be the first point of contact for supervisory authorities (the Information Commissioner's Office) and for individuals whose data is processed (colleagues, customers etc.), including the reporting of breaches and suspected breaches
- Quarterly and annual reporting on Data Protection activity to the Executive Team, Information Commissioners Office and Board respectively.

In particular the Data Protection & Information Officer is responsible for ensuring that appropriate procedures and guidance on our approach to data protection and privacy are available to Board members, leaders and colleagues.

7. BREACHES

A data breach can occur at any point when handling Personal Data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally to the Information Commissioner Office within 72 hours or the breach occurring or when Eildon become aware of the breach. .Such a breach will also need to be reported to the Board and Scottish Housing Regulator as a notifiable event.

Eildon take the security of data very seriously and will respond to any data breach in line with our Data breach procedure: here. All breaches will be recorded and notified to Executive Team.

8. DATA SUBJECT RIGHTS

Certain rights are provided to Data Subjects under Data Protection legislation:

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

Not all of these rights are absolute rights, and some are subject to qualification. A Data Subject may exercise one or more of these rights by submitting a request in writing to Eildon. Each request received by Eildon will require to be considered on its own merits and any specialist advice obtained, where appropriate, in relation to such requests from time to time. The DPIO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

Complaints

Where a Data Subject is unhappy with the way Eildon has dealt with their personal data and/or the exercising of their rights in relation to that data, the Data Subject should follow our Complaints Procedure, initially raising the complaint directly with the DPIO to allow the opportunity to rectify the situation.

If the Data Subject is dissatisfied with the outcome of the Eildon complaints process, they have the right to contact the Information Commissioner's Office to raise the matter with them.

9. FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

Eildon are also subject to the terms of the Freedom of Information (Scotland) Act 2002 ('FOISA') and the Environmental Information (Scotland) Regulations 2004 ('EIRs). This provides individuals with the right to request information that is held by Eildon. If a request was made under FOISA or EIRs for personal information, this information may be disclosed if the disclosure did not contravene any of the Data Protection principles. Eildon are fully committed to transparency and therefore will make every effort to meet the obligations of requests received and information will only be withheld where FOISA or EIRs permits the exception / exemption.

10. REVIEW OF POLICY

The Data & Information Officer will ensure this policy is reviewed every 3 years or earlier if there are any change to legislation. The Executive Team have delegated authority to approve and review this management policy.

APPENDIX - DEFINITIONS

Customer: anyone that Eildon processes personal data about, excluding employees. Including, but not limited to: tenants, factored properties, Border Care & Repair clients, Shared Owners, Mid Market Rent Tenancies, Complainants, Outreach clients, Applicants.

Data Controller: a person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

Data Processor: In relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the data controller.

Data Protection and Information Officer: someone within Eildon to take responsibility for data protection compliance.

Data Subject: a living individual who is the subject of personal data e.g. tenant, employee, board member, suppliers.

Information Commissioners Officer (ICO): Responsible for enforcing the Regulations.

Personal Data: Personal data is defined as, data relating to a living individual who can be identified from:

A) From those data;

B) From those data and other information, which is in the procession of, or is likely tocome into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing: in relation to information or data means obtaining, recording or holding the information or data or carrying out any operations or set of operations on the information or data.

Special Category Personal Data or Sensitive Personal Data: Personal data consisting of information as to:

- Racial, ethnic origin of the data subject
- Political opinions
- Religious beliefs, or other similar beliefs
- Member of a trade union
- Physical / mental health or conditions
- Sexual life
- Commission or alleged commission by the data subject of any offence
- Any proceedings for any offence committed or alleged to have been committed, disposal of proceedings, or sentence of any court in such proceedings.