Data Protection and GDPR Policy (Housing)

Policy Name:	Data Protection and GDPR Policy (Housing)
Version:	*V.1*
Approved by:	*The Board of Management and Trustees*
Approved date:	*17th November 2025*
Next review date:	*17th November 2026*
Key Legislation and Regulations:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Freedom of Information Act 2000 Oakfield also aligns with sector guidance from the Information Commissioner's Office (ICO) and best practices from leading housing providers ensuring that data protection is embedded in our culture and operations.
Relevant Policies:	Staff Training Complaints Whistleblowing Recruitment & Employment Safeguarding
EA:	Equality Analysis is currently under review
DPIA:	DPIA is currently under review
Consultation:	Board of Trustees
Applies to:	All Tenants, employees and volunteers

1. Policy Statement

Oakfield (Easton Maudit) Ltd is committed to protecting the personal data of everyone we work with—tenants, staff, volunteers, trustees, contractors, and community partners. We recognise that safeguarding privacy is not only a legal obligation but a reflection of our values: dignity, respect, and trust.

This policy outlines how Oakfield collects, uses, stores, and shares personal data in a lawful, fair, and transparent manner. It ensures that individuals' rights are upheld and that data is handled responsibly across all areas of our work.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with UK data protection legislation.
- Promote responsible data handling across Oakfield's operations.
- Protect the privacy rights of individuals interacting with Oakfield.
- Provide clear procedures for data access, correction, and breach response.

3. Scope

This policy applies to:

- Tenants and leaseholders
- Staff and volunteers
- Trustees and board members
- Contractors and service providers
- Any individual whose personal data is processed by Oakfield

It covers all personal data held in physical or digital formats, including housing records, employment files, support plans, and correspondence.

4. Data Protection Principles

Oakfield adheres to the following principles, as set out in the UK General Data Protection Regulation (UK GDPR):

- Lawfulness, Fairness, and Transparency - Data is collected and processed with a clear legal basis, and individuals are informed about how their data is used.
- Purpose Limitation - Data is only used for the specific purposes for which it was collected.
- Data Minimisation - Only the data necessary for the intended purpose is collected and retained.
- Accuracy - Data is kept accurate and up to date. Individuals can request corrections.
- Storage Limitation - Data is retained only for as long as necessary and securely disposed of when no longer needed.
- Integrity and Confidentiality - Data is stored securely, protected from unauthorised access, loss, or damage.
- Accountability - Oakfield takes responsibility for complying with data protection laws and demonstrating compliance.

5. Roles and Responsibilities

- **Data Protection Officer (DPO)** Oversees compliance, advises on data protection matters, and manages breach response.
- **Staff and Volunteers** Must handle personal data responsibly, follow procedures, and report any concerns or breaches.
- **Trustees** Ensure governance oversight and strategic accountability for data protection compliance.
- **Contractors and Third Parties** Must comply with Oakfield's data protection standards and contractual obligations.

6. Subject Access Requests (SARs)

Individuals have the right to:

- Request access to their personal data
- Request correction or deletion of inaccurate data
- Object to certain types of processing
- Request data portability (where applicable)

Oakfield will respond to SARs within one calendar month, unless an extension is justified. Requests must be submitted in writing and may require identity verification.

7. Data Breach Procedures

A data breach is any incident that results in:

- Unauthorised access to personal data
- Accidental loss or destruction of data
- Disclosure of data to unauthorised individuals

If a breach occurs:

- It must be reported immediately to the DPO
- A risk assessment will be conducted
- Affected individuals will be informed where appropriate
- The Information Commissioner's Office (ICO) will be notified if required

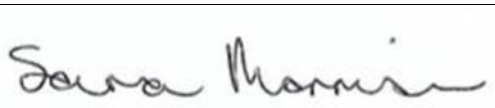
8. Confidentiality and Security Measures

Oakfield ensures:

- Password-protected systems and encrypted storage
- Secure disposal of paper records
- Restricted access to sensitive data
- Staff training on confidentiality and data handling
- Regular audits and reviews of data security protocols

9. Monitoring and Review

- The DPO will conduct annual reviews of data protection practices, and this is reviewed by the Managing Director.
- Trustees will receive regular updates on compliance and breaches.
- This policy will be reviewed annually or in response to legislative changes.

Signed – Chair of Trustees:	
Print:	Mrs Sara Morrison
Date:	17th November 2025