

DATA PROTECTION

POLICY AND PROCEDURE

Version Number: 3

Approval Date: November 2025

Approved by: Board

Next Review Date: September 2026

Responsible Officer: CEO

1.0 Introduction

- 1.1 HYELM is a charitable housing association providing affordable, high-quality accommodation for young professional people in London, especially those who might otherwise struggle to find safe, affordable housing.
- 1.2 As part of our work, HYELM processes personal data relating to tenants, staff, contractors, and others. This policy sets out how we protect that data and comply with our legal obligations.
- 1.3 HYELM is registered with the Information Commission (IC) as a Data Controller.
- 1.4 We are committed to promoting equality, accessibility, and transparency in all aspects of our data handling.

2.0 Definitions

- 2.1 **Personal Data** – Any information relating to an identified or identifiable living individual, such as name, identification number, location data, or other characteristics relating to their physical, physiological, genetic, mental, economic, cultural or social identity.
- 2.2 **Special Category Data** – Personal data that is more sensitive and needs more protection, including data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data (used for ID), and health or sexual orientation information.
- 2.3 **Processing** – Any action performed on personal data, whether manual or automated. This includes collecting, recording, storing, altering, retrieving, sharing, or deleting data.
- 2.4 **Data Subject** – The individual whose personal data is held or processed.
- 2.5 **Data Controller** – The organisation or person (HYELM) who decides how and why personal data is processed.
- 2.6 **Data Processor** – HYELM or a third party who processes personal data on behalf of HYELM, following our instructions.

- 2.7 **Personal Data Breach** – A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- 2.8 **Data Protection Impact Assessment (DPIA)** – A process that helps identify and reduce the data protection risks of a project or activity, especially where new or high-risk data processing is involved.
- 2.9 **Information Asset** – Any organised collection of personal data, whether digital or paper-based, such as spreadsheets, filing systems, databases, or shared drives.
- 2.10 **Legitimate Interest Assessment (LIA)** – A type of DPIA used to justify using legitimate interest as the lawful basis for processing personal data.
- 2.11 **Recognised Legitimate Interests** – Purposes recognised under the DUAA 2025 (fraud prevention, safeguarding, emergencies) where no Legitimate Interest Assessment is required.
- 2.12 **Consent** – Freely given, specific, informed and unambiguous agreement to the processing of personal data, signified by a clear affirmative action.
- 2.13 **Subject Access Request (SAR)** – A request made by a data subject to access the personal data held about them by a data controller.

3.0 Scope and Purpose

- 3.1 This policy applies to all personal data processed by HYELM, whether in electronic or hard copy format, relating to tenants, employees, board members, contractors, applicants, and service users.
- 3.2 This policy sets out how, as a responsible custodian of data, we'll manage, collect and process personal data in accordance with relevant data protection legislation and regulatory requirements.

4.0 Legal Framework

- 4.1 HYELM complies with the following legislation:
- The UK General Data Protection Regulation (UK GDPR)
 - The Data Protection Act 2018
 - Data (Use and Access) Act 2025

5.0 Principles

5.1 HYELM upholds the seven core principles underpinning data protection legislation. These principles guide all of our data handling activities:

- **Lawfulness, fairness and transparency** – We process data in a lawful, fair and open way, ensuring individuals understand how their data is used.
- **Purpose limitation** – We collect data only for specific, explicit and legitimate purposes and do not use it in ways that are incompatible with those purposes.
- **Data minimisation** – We only collect the data we need and no more.
- **Accuracy** – We take all reasonable steps to ensure personal data is accurate and kept up to date.
- **Storage limitation** – We keep data only for as long as necessary and dispose of it securely when no longer needed.
- **Integrity and confidentiality** – We protect data against unauthorised access, loss, or damage using appropriate technical and organisational measures.
- **Accountability** – We take responsibility for what we do with personal data and can demonstrate compliance with all of these principles.

6.0 Roles and Responsibilities

6.1 The Board

The Board has overall responsibility for ensuring the organisation complies with its legal obligations under data protection legislation. It will receive periodic assurance reports on compliance, breach activity, and policy review.

6.2 The Chief Executive Officer (CEO)

The CEO is responsible for overseeing the implementation of this policy and ensuring it is embedded in everyday operations. This includes ensuring all staff receive appropriate training, resourcing the role of the DPO, and monitoring any data protection risks at a senior level.

6.3 The Data Protection Officer (DPO)

HYELM's Finance Director is appointed as the DPO. The DPO is responsible for:

- Advising on data protection obligations and best practice
- Reviewing and signing off DPIAs
- Maintaining the Record of Processing Activities (ROPA)
- Logging and investigating any data breaches
- Coordinating responses to Subject Access Requests (SARs)
- Leading annual data retention reviews
- Overseeing processor contracts and data sharing agreements
- Acting as the first point of contact for the Information Commissioner's Office (ICO)

6.4 All Staff

All HYELM staff are responsible for:

- Following data protection policies and procedures

- Completing training as required
- Reporting suspected or actual breaches without delay
- Ensuring the accuracy and security of personal data they handle

7.0 Lawful basis for Processing

- 7.1 HYELM will process data only where a lawful basis applies: consent, contract, legal obligation, vital interests, public task, or legitimate interest (including recognised legitimate interests under DUAA 2025).

8.0 Individual Rights

- 8.1 Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, individuals have a set of rights over their personal data. These rights are designed to give people greater control, transparency and protection in relation to how their personal information is used. The Data (Use and Access) Act 2025 (DUAA) has updated some aspects of these rights, but the underlying principles remain the same. HYELM is committed to ensuring that these rights can be exercised fairly and without unnecessary barriers.

8.2 Right of Access

- An individual has the right to request a copy of the personal information that HYELM holds about them. This is known as making a Subject Access Request (SAR).
- The request will normally be fulfilled within one month, although this period can be extended if the request is complex.
- Under DUAA, if HYELM requires clarification to locate the relevant information, the time limit will be paused until clarification is received.

8.3 Right to Rectification

- If information held by HYELM is inaccurate or incomplete, an individual has the right to request that it is corrected or updated.
- HYELM will respond to requests for rectification promptly and will take all reasonable steps to verify the accuracy of the updated information.

8.4 Right to Erasure (Right to be Forgotten)

- An individual may request that their personal data is deleted when it is no longer needed for the purpose it was collected, or if consent has been withdrawn where consent was the lawful basis for processing.
- HYELM will comply with requests for erasure wherever possible, although in some cases data may need to be retained to meet legal or contractual obligations.
- If data cannot be erased, HYELM will explain the reasons clearly to the individual.

8.5 Right to Restriction of Processing

- In certain circumstances, an individual can ask HYELM to limit how their information is used.
- This may apply if the accuracy of the data is contested or if the individual wants HYELM to keep the information but not use it while a concern is being resolved.
- In such cases, the data will continue to be stored securely but will not normally be used until the restriction is lifted.

8.6 Right to Data Portability

- Where personal data has been provided directly by an individual and is processed based on consent or contract, and by automated means, the individual has the right to request a copy of that data in a structured, commonly used and machine-readable format.
- An individual may also request that HYELM transfers it directly to another organisation.

8.7 Right to Object

- An individual has the right to object to their personal data being used for particular purposes.
- The most common example is direct marketing, which must stop immediately if an objection is raised.
- In other cases, such as when HYELM relies on legitimate interests, the organisation may be able to continue processing if it can demonstrate compelling and lawful reasons that override the individual's objection.

8.8 Rights in Relation to Automated Decision-Making and Profiling

- Individuals have the right not to be subject to decisions made solely by automated systems if those decisions have significant effects, such as impacting their access to services.
- Where HYELM uses any form of automated decision-making, safeguards will be in place to ensure transparency, the involvement of human oversight, and the opportunity for individuals to request that a decision is reviewed by a member of staff.

9.0 Subject Access Requests (SARS)

9.1 Under UK GDPR, the Data Protection Act 2018, and the DUAA 2025, any individual has the right to ask HYELM for a copy of the personal data held about them. This is called making a Subject Access Request (SAR). HYELM is committed to handling all SARs in a fair, proportionate, and timely way.

9.2 Submitting a Request

- A SAR can be made in writing (by email or letter) or verbally (in person or by telephone).

- All staff who receive a SAR verbally must record the details in writing and pass it immediately to the CEO.
- SARs can be submitted to HYELM via email, letter or verbal request.

9.3 The DPO will be responsible for logging the request in HYELM's SAR Register and for coordinating the response.

9.4 Acknowledging Requests

- All SARs will be recorded and then acknowledged within five working days of receipt.
- If clarification is required to identify the relevant information, HYELM will contact the individual promptly.

9.5 Responding to Requests

- HYELM will normally provide the information within one calendar month of receiving the request (or clarification, if required).
- For complex or multiple requests, HYELM may extend the deadline by up to two additional months. The individual will be informed of any extension within the first month, along with the reasons for it.
- Responses will be proportionate and reasonable. HYELM will not be required to search for or disclose irrelevant or excessive data.
- If the request relates to CCTV data, then HYELM may be unable to provide this if the data requested also contains data related to a third party (e.g. another resident, contractor, visitor etc).
- If the data requested is in relation to criminal / illegal activity then HYELM can provide this directly to a law enforcement agency where we have received an official data request.

9.6 Format of Information Provided

- Information will be provided securely, in a clear and accessible format.
- Where an individual makes a request electronically, the response will normally be provided in a commonly used electronic format, unless otherwise requested.

9.7 Oversight and Record-Keeping

- The DPO will maintain a SAR Register recording the date of request, requester's details, actions taken, and deadlines.
- Records will be used to monitor compliance with statutory timescales and to identify any recurring issues.

10.0 Data Accuracy

10.1 HYELM will take all reasonable steps to ensure that personal data is accurate and up to date.

10.2 Staff will:

- Confirm personal details at tenancy reviews using a tenancy review form.
- Confirm personal details each year when P60 forms are issued.
- Use everyday contact with tenants as an opportunity to check and update records.

10.3 HYELM will maintain housing management policies to ensure accuracy checks are built into tenancy reviews and staff guidance.

11.0 Data Retention, Review And Disposal

11.1 HYELM will only retain personal data for as long as it is needed to fulfil the purpose for which it was collected, or to meet legal, contractual, or regulatory requirements.

11.2 HYELM maintains a formal Retention Schedule, which sets out how long different categories of records will be kept. Examples include:

- Tenancy Agreements: 6 years after tenancy ends.
- Financial Records: 7 years.
- HR/Staff Records: 6 years after employment ends.
- Safeguarding Records: 10 years, or longer if the case remains active.
- CCTV Footage: 30 days unless required for an investigation.
- Complaints: 6 years.

11.3 HYELM's programme for reviewing and disposing of data consists of:

- **Annual Review Cycle:** each year, the DPO will lead a review of data held in hard copy and electronically, comparing it against the Retention Schedule.
- **Team Responsibility:** Members of the team have responsibility for flagging records due for review or deletion and will have deletion tasks assigned to them.
- **Central Oversight:** the DPO will coordinate and maintain a log of reviews and disposals.

11.4 Process for Reviewing Data:

- At the start of each financial year, a retention review timetable will be agreed.
- Data categories approaching their retention limit will be identified.
- DPO will check if there is a continuing lawful basis to retain the data (e.g. ongoing tenancy, unresolved complaint, legal hold).
- If no lawful basis exists, the data will be scheduled for secure deletion or disposal.

11.5 Process for Disposing of Data:

- Paper records will be destroyed by cross-cut shredding or via an accredited confidential waste contractor. Certificates of destruction will be obtained and retained.
- Electronic records will be permanently deleted from systems and backups, using IT-secure deletion methods. Where deletion is not technically possible, records will be anonymised so individuals are no longer identifiable.
- CCTV Footage is automatically overwritten after 30 days unless flagged for investigation.

11.6 Recording and Monitoring:

- A Retention and Disposal Log will be maintained, recording category of data, date of review, action taken, method of disposal, and staff responsible.
- The log will be reviewed annually by the DPO and CEO and presented to the Board for assurance.
- Staff will receive training on the Retention Schedule and disposal procedures.
- Appendix D provides a summary of retention periods. The full detailed Retention Schedule is maintained separately and will be updated regularly in line with changes to legislation and regulatory guidance.

12.0 Data Security

12.1 HYELM uses encrypted systems, access controls and secure servers.

12.2 Staff are responsible for:

- Securing work devices
- Locking screens when unattended
- Not sharing passwords
- Only accessing data they are authorised to use

12.3 HYELM will undertake regular reviews of its IT and data protection infrastructure.

13.0 Data Breaches

13.1 A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

13.2 Examples include:

- Sending personal information to the wrong recipient (e.g. emailing the wrong person)
- Sharing information about a resident without written consent to do so
- Loss or theft of devices or hard copy files
- Hacking or malware attacks
- Unauthorised access to records by staff or third parties

13.3 All staff must report actual or suspected breaches immediately to the Housing Manager who will log the incident and identify individuals affected, then report to the DPO.

13.4 The DPO will:

- Investigate the cause and extent
- Assess the level of risk



- Report to the CEO

- 13.5 If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO or the CEO will notify the IC within 72 hours and, where necessary, inform those affected.
- 13.6 A record will be kept of all breaches, regardless of whether they are reported to the IC.
- 13.7 See Appendix A – Data Breach Response Flowchart.

14.0 Data Protection Impact Assessments (DPIAs)

- 14.1 HYELM will adopt a risk-based approach to processing personal data, ensuring that any risks to privacy or to the rights and freedoms of individuals are assessed before starting, commissioning, or changing data processing activities.
- 14.2 A Data Protection Impact Assessment (DPIA) will be carried out whenever HYELM plans to introduce or change:
- A new or revised policy involving personal data.
 - A new or changing data processing activity.
 - A new or changing system within which data is held.
 - A new or changing data sharing activity.
- 14.3 The purpose of a DPIA is to:
- Identify potential risks to individuals.
 - Assess whether the planned processing is necessary and proportionate.
 - Put in place measures to reduce or remove risks where possible.
- 14.4 HYELM will use its approved DPIA template (Appendix B) to complete all assessments. This template ensures that risks to individuals are clearly documented, along with the safeguards and actions taken to manage those risks.
- 14.5 The DPO is responsible for maintaining a central log and ensuring they are updated when activities change. The CEO is responsible for reviewing all DPIAs.
- 14.6 If a DPIA shows that risks cannot be reduced to an acceptable level, HYELM will consult with the Information Commission before proceeding.

15.0 Third Party processing

- 15.1 HYELM will only engage processors who provide sufficient guarantees about their compliance with UK GDPR.
- 15.2 All processing relationships will be governed by a written data processing agreement.

15.3 HYELM will maintain a record of all data processors and review contracts regularly.

16.0 DATA MAPPING

16.1 HYELM will maintain a Record of Processing Activities (ROPA) in line with Article 30 of UK GDPR.

16.2 This will include details of:

- Data categories
- Data subjects
- Processing purposes
- Data recipients
- Retention periods
- Technical and organisational security measures

16.3 The data mapping spreadsheet will be reviewed at least every 5 years and updated after major changes. The spreadsheet will record the date of last review and responsible staff.

17.0 TRAINING AND AWARENESS

17.1 All new staff will receive data protection training as part of their induction.

17.2 Refresher training will be delivered every three years or sooner if legislation or HYELM's processes change.

17.3 Completion of training will be monitored by the CEO.

18.0 Linked Docs:

- AI policy
- Tenancy Review Form
- CCTV policy
- IT Policy
- Privacy Notices

19.0 APPENDICES

- Appendix A: Data Breach Response Flowchart
- Appendix B: DPIA Template

- Appendix C: Privacy Notice Template
- Appendix D: Summary Data Retention Schedule



Version Control Table

Status (draft/ approved)	Version #	Date	Amendments
Approved	3	Nov 2025	Reformatted Inclusion of data retention schedule More detailed procedure for response to data breach
Approved	2	June 2020	Revised to comply with GDPR