

DATA PROTECTION POLICY

UK GDPR and Data Protection Act 2018

TABLE OF CONTENTS

Quality Standards.....	3
Key Principles.....	3
Policy Statement.....	4
Legislative Framework.....	4
Procedure.....	4
Training and Development.....	6
Monitoring and Review.....	6
Appendix A: Retention Schedule.....	7
Appendix B: Data Breach Log.....	8
Authorisation and Signature.....	8

Quality Standards

Solace Housing holds personal information about residents, staff, referrers, landlords and contractors, including sensitive information about health, safeguarding, offending and finances. Solace Housing is committed to handling all personal information lawfully, fairly, securely and with respect for people's privacy and dignity. This policy sets out how Solace Housing complies with data protection law.

To achieve this, Solace Housing will ensure that:

Lawful, Fair and Transparent

Personal information is only used where there is a lawful basis, and people are told how it is used through privacy notices.

Confidential and Secure

Access is limited to those who need it, and information is protected by physical, technical and organisational security.

Accurate and Kept Only as Long as Needed

Information is kept accurate and up to date and is securely destroyed in line with the retention schedule.

Rights Are Respected

Requests from individuals, including subject access requests, are handled within legal timescales.

Breaches Are Managed

Data breaches are reported, investigated and, where required, notified to the ICO within 72 hours.

Staff Are Trained

All staff complete data protection training at induction and every year.

Key Principles

Solace Housing follows the seven UK GDPR principles. Personal data must be processed lawfully, fairly and transparently; collected for specified and legitimate purposes; limited to what is necessary; accurate and up to date; kept no longer than necessary; kept secure; and handled in a way Solace Housing can show complies (accountability).

Policy Statement

Solace Housing Ltd is the data controller and is registered with the Information Commissioner's Office (BVSC-148). The Directors have overall responsibility for this policy. The Company Director and Head of HR acts as the Data Protection Lead, handling requests, breaches and advice. All staff, agency workers, volunteers and contractors must follow this policy.

Legislative Framework

This document has been developed with reference to current legislation, statutory guidance and recognised good practice, including but not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Human Rights Act 1998, Article 8 (right to respect for private and family life)
- Common law duty of confidentiality
- Care Act 2014 (information sharing to safeguard adults)
- ICO guidance and codes of practice
- Health and Safety at Work etc. Act 1974
- Supported Housing (Regulatory Oversight) Act 2023 and the National Supported Housing Standards

Procedure

1. Collecting Information

Only information that is needed is collected. Before collecting it, staff make sure there is a lawful basis and give the person the relevant privacy notice (residents at sign up, staff at recruitment). Special category data (such as health) and criminal offence data are only collected where there is an extra legal condition, as recorded in the Data Protection Impact Assessment (BVSC-147).

2. Using Information

Information is used only for the purpose it was collected for, such as referrals, housing management, support, safeguarding, risk assessment, employment, finance and regulatory compliance. Any new use must be approved by the Data Protection Lead.

3. Security

- Password protected systems, with multi-factor authentication where available.
- Encrypted devices, automatic screen locking and secure email.
- Paper records in locked cabinets, and a controlled office.
- Confidential waste shredded or securely destroyed.
- Systems kept updated, with regular backups.

- No personal data on personal devices or personal email accounts.

4. Confidentiality and Access

Staff only access records they need for their role. Looking at records out of curiosity, or sharing information without authority, is a disciplinary matter.

5. Sharing Information

Information is shared only where there is a lawful basis, such as consent, a contract, a legal duty, or to protect someone from serious harm. Sharing follows the Data Sharing Protocol (BVSC-145) and Data Sharing Agreement with Residents (BVSC-144). Processors such as IT providers have a written Data Processing Agreement (BVSC-149). In an emergency or safeguarding situation, information is shared to protect life, and the reason is recorded.

6. Individuals' Rights

People have the right to be informed, to access their data, to have it corrected, erased or restricted, to object, and to data portability, where these rights apply. Requests can be made verbally or in writing to any member of staff and are passed to the Data Protection Lead the same day.

7. Subject Access Requests

1. The request is logged and the person's identity is checked.
2. A reasonable and proportionate search is made for their information.
3. Other people's information is removed unless they agree or it is reasonable to share it.
4. A response is given within one month, which can be extended by up to two months for complex requests. The person is told of any extension within the first month.
5. Requests are free unless they are clearly unfounded or excessive.

8. Retention and Disposal

Records are kept only as long as set out in the Retention Schedule (Appendix A), then securely destroyed.

9. Data Breaches

1. Any actual or suspected breach, such as an email to the wrong person, a lost phone or a stolen file, is reported to the Data Protection Lead immediately.
2. The breach is contained, and the risk to people is assessed.
3. If there is a risk to people's rights and freedoms, the ICO is told within 72 hours of Solace Housing becoming aware.
4. If the risk is high, the people affected are told without undue delay.
5. All breaches, including those not reported to the ICO, are recorded in the Breach Log (Appendix B), and lessons are learned.

10. Data Protection Complaints

Anyone can complain to Solace Housing about how their information has been handled. Complaints are acknowledged within 30 days and investigated without undue delay. People also have the right to complain to the ICO (ico.org.uk, 0303 123 1113).

11. CCTV and Data Protection Impact Assessments

CCTV is managed under the CCTV Policy (BVSC-146). A Data Protection Impact Assessment (BVSC-147) is completed before any new high risk processing, such as new systems or new ways of sharing data.

Training and Development

All staff complete Cyber Security and Data Protection training before using Solace Housing systems, and refresh it every year (BVSC-040). Staff who handle requests and breaches receive further guidance from the Data Protection Lead.

Monitoring and Review

Compliance will be monitored through the quality assurance framework set out in the Quality Assurance Policy (SH002). Monitoring activities will include:

- Annual data protection audit, including access controls and records.
- Review of subject access requests and response times.
- Review of the Breach Log every quarter.
- Annual check of ICO registration.

The ICO registration, privacy notices, Breach Log, subject access request log, training records and Data Protection Impact Assessments are the evidence locations for audit purposes. Findings will be reported to the Directors and shared with the Registered Provider where required, and any gaps will be addressed through a Quality Improvement Plan. This document will be reviewed at least annually, or sooner where legislation, guidance or audit findings indicate that a review is necessary.

Appendix A: Retention Schedule

Record	Keep For	Then
Resident files (support, licence, risk)	6 years after the resident leaves	Secure destruction
Safeguarding records	6 years after the resident leaves, or longer if there is an ongoing investigation or legal claim	Review, then secure destruction
Referral forms where the person did not move in	1 year after the decision	Secure destruction
Rent, service charge and finance records	6 years after the end of the financial year	Secure destruction
Staff personnel files	6 years after employment ends	Secure destruction
Unsuccessful job applications	6 months after the decision	Secure destruction
DBS certificates	Not kept. Record the certificate number, date and decision only	Destroy certificate copies within 6 months
Right to work documents	2 years after employment ends	Secure destruction
Payroll and tax records	6 years after the end of the tax year	Secure destruction
Accident book and RIDDOR records	At least 3 years after the entry	Secure destruction
Property compliance certificates	For the life of the property under management, plus 6 years	Secure destruction
CCTV footage	30 days unless needed for an investigation	Automatic overwrite

Appendix B: Data Breach Log

Date	What Happened	People Affected	Risk (L / M / H)	Reported to ICO?	Action Taken

Authorisation and Signature

This Policy is the authorised version agreed by the Directors of Solace Housing.

All employees are expected to follow this policy and failure to do so could result in disciplinary action.



Signed on behalf of Solace Housing.