

General Data Protection Regulation (GDPR) Policy

DRAFT - under consultation (end: 01/10/2026)

Introduction

Our mission is to improve the quality of life for our residents.

Handling of data is an important priority and duty for Spitalfields Housing Association (SHA). We engage with our stakeholders in a range of ways and records must be kept up to date. These transactions require processing information. We are legally obliged to fulfil responsibilities to ensure appropriate safeguards and standards are set out and maintained.

We have a duty to maintain confidentiality in all aspects of our work. Staff will have access to information on a need to know basis. Personal information will only be shared where there is a legitimate business need, appropriate authorisation, and a lawful basis for disclosure.

Purpose

This policy outlines our commitment to ensuring we handle data in accordance with the UK General Data Protection Regulation (UK GDPR) which took effect in May 2018, and the UK Data Protection Act (DPA) 2018. This requires personal information to be processed fairly, for limited purposes, relevantly, accurately, not kept longer than necessary, in line with people's rights, kept securely and not to be transferred outside of the UK unless appropriate safeguards are in place, in accordance with UK GDPR.

Scope

UK GDPR applies to information relating to identified or identifiable living individuals. The policy applies to all aspects of our work covering staff employment, current, former and future residents' records. Information on computers, paper, audio and video all fall within the scope of the policy. It also applies to other stakeholders where we process information. This includes Board members, staff, volunteers and residents who have access to records.

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

SHA is responsible for demonstrating compliance with UK GDPR and will maintain appropriate records, policies, procedures, training, audits, and governance arrangements to evidence that personal data is processed lawfully, fairly, transparently and securely.

Privacy Notice

For customers, residents and tenants

The Privacy Notice included here to explain how the organisation collects and processes personal information in order to conduct normal business activities as a UK housing association. This Privacy Notice tells you what to expect when SHA processes personal information. It applies to information about applicants, residents and other service users. It tells you the purposes for which we may process your personal information and the legal basis for processing this information.

SHA may collect a range of personal information from residents to manage tenancies, provide housing services, meet legal obligations, and support resident wellbeing. This can include: personal details, contact information, household information, housing and tenancy information, financial information, support and wellbeing information, equality, diversity and inclusion information, communication records, and security information.

Special category information (such as health, ethnicity, or religion) is usually collected only where there is a lawful basis and a clear need to do so.

Our Privacy Notice explains:

- what personal information we collect;
- why we collect it;
- our lawful basis for processing;
- who we share information with;
- how long we keep information;
- any international transfers;
- individuals' rights and how to exercise them;

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

- how to complain to SHA and the ICO.

Who we are

SHA is a data controller of personal information for the purposes of the UK GDPR. Our contact details for data protection purposes are as follows:

Spitalfields Housing Association
1 Canada Square
London
E14 5AB

Telephone: 020 7392 5400

Email: admin@spitalfieldsha.co.uk

SHA has assessed its processing activities against the requirements of Article 37 UK GDPR and has determined that a Data Protection Officer (DPO) is not legally required. SHA has appointed Data Protection Leads (DPLs) to oversee compliance, provide advice, monitor data protection risks and act as a point of contact for data protection matters.

Internal policy

For staff, board members and volunteers

SHA will:

- comply with the seven data protection principles - see table below.
- maintain confidentiality of all personal data held by us on a need to know basis.
- ensure that personal data is accurate and up to date.
- securely destroy data to ensure information is not kept longer than needed.
- set up information sharing protocols in dealing with anti-social behaviour and other services within a multi-agency forum.
- provide staff with training, support and guidance in fulfilling our responsibilities.
- investigate all breaches and take disciplinary action against staff who fail to comply with the policy.
- deal promptly with personal data requests, including for a Subject Access Request (SAR) free of charge.
- Where data requests are deemed manifestly unfounded, highly repetitive,

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

excessive or extra copies are requested, SHA may charge a reasonable fee based on the administrative costs of complying with a request where permitted by UK GDPR. Requesters will be notified of this at the time.

- ensure registration with the Information Commissioner's Office (ICO) is kept up to date.
- get appropriate levels of consent when disclosing information to third parties.
- comply with exemptions in the act, and withhold third party data from individuals who do not have a right to see such information.
- train new staff and volunteers in the Policy at their induction to fulfil their contractual obligations, and to include it in the staff handbook.

Seven UK GDPR principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Responsibility & Accountability

The designated DPL(s) will ensure compliance with the policy, provide procedures for staff and oversee reviews. All staff are responsible for implementing this policy to best practice standards.

Personal data breaches must be reported immediately to the DPL. SHA will assess all data breaches, record them in the breach register, take steps to reduce harm and notify affected individuals where required. Where a breach is likely to result in a risk to individuals' rights and freedoms, SHA will notify the ICO within 72 hours where required. The DPL will have access to senior management, act with freedom from instruction, and be protected from penalty in acting on their statutory duties (in line with Articles 37-39 of UK GDPR)

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

Review & Evaluation

All department managers have a duty to ensure the policy is adhered to, and instruct and monitor staff, where appropriate.

Why do we collect and store personal information?

SHA processes personal information to enable us to provide social housing accommodation and services, which include:

- Letting, renting and leasing properties
- Administering waiting lists
- Carrying out research
- Administering housing and property grants
- Providing associated welfare services, advice and support
- Maintaining our accounts and records
- Maintaining and managing our employees, agents and contractors

We also process personal information using CCTV systems to monitor and collect visual images for the purpose of security and the prevention and detection of crime.

Legal basis for processing

SHA will only collect and process your personal data under the UK GDPR where the following conditions have been met:

- The processing is necessary for the performance of a contract we have with you;
- The processing is necessary under a legal obligation;
- The processing is necessary where we need to protect the vital interests (i.e. health and safety) of you or another person;
- The processing is necessary where we need to perform a task in the public interest;
- legitimate interests as a social housing provider, where processing is necessary to manage services, protect residents, maintain safe communities, prevent fraud, manage risks and improve service delivery, provided these interests do not override individuals' rights and freedoms.

Special Category data

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

Some personal information is treated as more sensitive (such as health, sexuality, ethnic background – see footnote below for further explanation [1]). The legal basis for processing personal information is more limited. The reasons we can use are:

- Where we need to protect the vital interests (i.e. health and safety) of you or another person;
- Where you have already made your personal information public;
- Where we or another person needs to bring or defend legal claims;
- Substantial public interest grounds;
- Where it is deemed in SHA's legitimate interests, a Legitimate Interest Assessment (LIA) is to be undertaken, consisting of: defining the interest, assessing necessity, assessing balance against individual rights, document decisions, and add safeguards where necessary;
- Where Special Category data is sought, this will be collected in line with Article 9 and Schedule 1 of DPA 2018, overseen by a DPL in the form of an appropriate Policy Document (APD) for Special Category data retention.

Any legitimate interests pursued by us, or third parties we use, are as follows:

Equal opportunities monitoring: We collect protected characteristic data such as your gender, ethnicity, and sexuality to monitor the effectiveness of our equal opportunities policy. This is important for ensuring our services do not exclude certain disadvantaged groups and helps to ensure we are an inclusive housing association.

Safeguarding purposes: We collect certain personal information to implement appropriate safeguarding measures for our residents and employees and to provide efficient service delivery and planning.

To provide adequate support: We collect information such as your employment status and access to public funds so that we can assess residents' needs and suitability of services. This information also helps us to make appropriate adaptations to the home, to make appropriate referrals, to allow for appropriate communications, and to allow for appropriate repairs and customer care.

How we collect your information

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

SHA collects information from you via a variety of sources, including when you apply for one of our properties or services, complete one of our forms, when you call, write, email or meet with us or respond to a survey. SHA operates a CCTV system to provide a safe and secure environment for residents and visitors and to protect its property. We use CCTV to detect alleged anti-social behaviour or crime, monitor security of premises and breach of tenancy agreements.

Recorded images will automatically be overwritten after a period no longer than 30 days. If an image/s has been stored for evidential purposes and is no longer required, it will be destroyed in an appropriate manner. We may record phone calls for training and quality purposes. Records may be kept longer, if forming as part of an investigation.

What information we collect from you

The information we collect and may hold from you on a lawful basis may include:

- Names and date of birth, proof of identity
- Contact details so we can communicate with you by your preferred means, and keep you informed about services we offer which may be useful to you
- National Insurance number
- Bank statements, payslips or income details required for processing your tenancy application
- We keep financial information obtained through rent account details, including credit history and benefits information. We may use this to help resolve arrears payments and optionally to provide welfare, benefits and debt advice as a free service to help you budget and pay your bills.
- Special categories of information such as race, gender, ethnic origin, and sexuality for our equality monitoring purposes.
- Information on disabilities, vulnerabilities and special needs to tailor our service to better meet your particular circumstances and needs. We may use this information for safeguarding of staff.
- We collect your education and employment details to use for our training and employment services.
- We record health, safety and security details.

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

This is not an exhaustive list as we hold records of most contacts we have with you, or about you, and we process this information so we can deliver services to you. Generally the information we hold will have been provided by you (on application or enquiry forms or when we communicate with you), but we may also hold information provided by third parties where this is relevant to your housing circumstances.

The lawful basis for collecting and holding data are reasons such as legitimate interest, relating to contracts, legal obligations and public tasks, as exemplified below:

Processing activity	Lawful basis	Retention schedule
Tenancy management	Contract (Art. 6(1)(b))	6 years
Rent collection	Contract / Legal obligation	6 years
Safeguarding	Vital interests / Substantial public interest	6 years
Financial records	Contract / Legal obligation	6 years
Equality monitoring	Art. 9 condition + Schedule 1 DPA 2018	2 years
CCTV	Legitimate interests	30 days (longer for any investigations)
Complaint	Legal obligation (Limitation Act 1980)	6 years
Recruitment records	Legitimate interests	12 months

Retention periods are reviewed periodically by DPLs.

How we manage your personal information

SHA processes your personal information in accordance with the principles of UK GDPR. We will treat your personal information fairly and lawfully and we will ensure that information is:

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

- Processed for limited purposes;
- Kept up-to-date, accurate, relevant and not excessive;
- Not kept longer than is necessary;
- Kept secure;
- Access to personal information is restricted to authorised individuals on a strictly need to know basis.

We are committed to keeping your personal details up to date, and we encourage you to inform us about any changes needed to ensure your details are accurate. SHA uses a range of IT systems to store personal data and we maintain these to ensure they are secure and to comply with UK GDPR standards. SHA does not currently make solely automated decisions with legal or similarly significant effects. If SHA introduces new systems and measures, this will be subject to appropriate safeguards, and individuals will be informed of their rights.

Data at the first instance is held within the UK, and any transfers outside of the UK must meet adequacy regulations, to comply with with Chapter V (UK GDPR), International Data Transfer Agreements (IDTAs), UK Addendum to the EU Standard Contractual Clauses (SCCs), and any processor obligations for overseas access.

Secure systems of data protection can include: multi-factor authentication, encryption at rest and in transit, access logging, role-based access controls. SHA will implement secure disposal procedures, and periodic penetration testing and vulnerability management.

How long we store your personal information

SHA will retain personal information only for as long as necessary for the purpose it was collected, taking account of legal, regulatory, contractual and operational requirements. Retention periods are documented in SHA's retention schedule and reviewed regularly.

Who we may share your information with

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of UK GDPR. Requests from outside organisations for information about residents must be in writing unless there are good reasons for the matter to be dealt with orally, eg. an urgent request from the police where somebody's

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

health or safety is at risk. Such situations will be rare and SHA will use its discretion to consider where such disclosure would be appropriate in the circumstances. SHA will ensure the safeguarding of its residents' rights is considered when approached by an outside agency with a request for information. SHA will only share personal data where there is a lawful basis, a clear purpose, and the sharing is necessary and proportionate. Where another organisation processes personal data on behalf of SHA, appropriate written agreements meeting Article 28 UK GDPR requirements will be in place. Information sharing decisions will be documented where appropriate.

The following is a list of the types of organisations we may need to share some of the personal information we process with for one or more reasons:

- Family, associates and representatives
- Suppliers and service providers
- Financial organisations
- Central government for housing benefits, universal credit, social services, and housing options
- CORE (COntinuous REcording of Lettings and Sales in Social Housing in England)
- Other housing associations or trusts
- Health authorities
- Health and social welfare organisations
- Security organisations
- Charities and voluntary organisations
- Police forces
- Food banks
- Courts and tribunals
- Employment and recruitment agencies
- Credit reference agencies
- Debt collection agencies
- Other social landlords
- Capita
- PSC Systems
- Our contractors

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

Our Data Protection procedure

Where applicable, SHA's DPLs will undertake the following activities to support compliance with this policy:

- Understand key data protection terms and follow organisational guidance.
- Complete a Data Protection Impact Assessment (DPIA) for new or high-risk processing activities and significant changes [2]
- Maintain Records of Processing Activities (ROPA), identifying processing purposes, categories of personal data, lawful bases, recipients, retention periods and security measures.
- Respond promptly to individual rights requests in line with procedures.
- Report and manage all actual or suspected data breaches immediately.
- Retain and dispose of personal data in accordance with retention schedules.
- Ensure CCTV use complies with organisational policy.
- Share personal data only where lawful, necessary, and documented.
- Conduct due diligence on processors and monitor compliance.
- Apply data protection by design and default by considering privacy risks at the earliest stage of any new project, system, service or change in processing activity. (Privacy-friendly settings are automatically applied as the standard)
- Use enhanced safeguards when processing children's data, and vulnerable adults.
- Promote equality, diversity, and fair treatment in all data protection activities.

Your rights

Under the GDPR, you have the right to ask us what personal information we hold, and to request a copy of this information. You can email your request to us at admin@spitalfieldsha.co.uk. Subject Access Requests will normally be provided free of charge. SHA may charge a reasonable fee or refuse a request where it is manifestly unfounded or excessive, in accordance with UK GDPR. We have one calendar month within which to provide you with the information you have requested for. Following your request, we will provide you with a copy of the information we hold that relates to you.

You have the right to correct any mistakes contained in the information we hold about you. Please advise us of any changes or corrections by contacting us at

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

admin@spitalfieldsha.co.uk or by using the 'Inform us of change' online form via the SHA website. You also have the right to:

- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- object to processing where we say it is in our legitimate business interests, unless we can show there is a compelling legitimate reason for the processing
- Restrict us from processing your personal information
- Right to data portability
- Right to withdraw consent
- Rights relating to automated decision-making and profiling
- Right to be informed

Children and vulnerable adults

SHA recognises that children and vulnerable adults may require additional protection. Processing involving these groups will consider their best interests, dignity, privacy and ability to understand how their information is used. Information will be provided in an accessible format, with reasonable adjustments made where required. Data collection will be limited to what is necessary, and profiling or processing likely to cause harm will be avoided. Carers, guardians or representatives will only be involved where appropriate and lawful.

The right to make a complaint & the Information Commissioner's Office (ICO)

You have the right to complain, ask a question or make a request about any matter relating to our service, including how we use your personal data. In the first instance, please contact SHA by email at admin@spitalfieldsha.co.uk

Before making a complaint to the ICO, you should make a formal complaint to SHA. The complaints process and policy can be found on the SHA website (spitalfieldsha.co.uk) You have the right to complain to the ICO if you think we have breached UK GDPR rules. ICO contact details are given below.

Address: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Telephone: 0303 123 1113

GDPR Policy

DRAFT - under consultation (end: 01/10/2026)

Website: ico.org.uk

[1] List of special categories are defined within UK GDPR and include race, ethnic origin, politics, religion, trade union membership, genetics, biometric data, health, sex life, or sexual orientation. Where SHA processes special category data, it will identify both an Article 6 lawful basis and an Article 9 condition under UK GDPR, together with any applicable Schedule 1 condition under the Data Protection Act 2018. Appropriate safeguards, including access controls, retention limits and an Appropriate Policy Document (APD) where required, will be maintained.

[2] DPIAs will be completed where processing is likely to result in a high risk to individuals, including large-scale processing of special category data, systematic monitoring, significant profiling, new technologies, or processing involving vulnerable groups.

We refer to the resident, tenant or customer meaning a person residing in an SHA-managed property.

We welcome the views of customers in improving the services we provide. Customers can give feedback through our online feedback form via the SHA website: www.spitalfieldsha.co.uk