Islington & Shoreditch Housing Association

DATA PROTECTION POLICY

1. SCOPE

This policy sets out ISHA's commitment and approach to data protection and provides guidance to meet our standards, aims and ideals with respect to data protection compliance. It applies to all of ISHA's activities and operations which involve the processing of personal data. It applies to anyone who processes personal data for or on behalf of ISHA, including: employees, casual and temporary staff, board and committee members, involved residents, volunteers and third-parties such as sub-contractors and suppliers or anyone who ISHA shares or discloses personal data with/to. It also applies where ISHA is a joint controller or, where relevant, acts as a processor for another controller.

2. STATUTORY AND REGULATORY FRAMEWORK

The processing of personal data in the UK is regulated by law, principally,

- The UK General Data Protection Regulation (UK GDPR); and
- The Data Protection Act ("DPA") 2018

The DPA sits alongside and supplements the UK GDPR. Other laws inter-relate with the DPA and the UK GDPR, including, but not limited to, the Privacy and Electronic Communications Regulations (2003) ("PECR").

Together, this Data Protection Legislation sets out legal responsibilities on all organisations processing personal data and makes clear the rights of those people whose data is being processed. It is extremely important that ISHA is compliant with legislation. Penalties can be imposed on organisations inadequately processing personal data, including fines of up to £17.5 million (or 4% of global annual turnover, whichever is higher). Individuals can also be held accountable under the legislation and sentenced by the courts for offences.

Roles and responsibilities are outlined in Section 4. The Appendix provides definitions of the terms used in this Policy.

3. OUR APPROACH

ISHA's Board and Leadership Team are committed to compliance with all relevant Data Protection Legislation and will delegate appropriate powers and responsibilities to its staff to ensure it is fully compliant. ISHA will ensure legal compliance with relevant data protection legislation. These documents will be regularly reviewed (at least every 3 years or earlier if legislation requires it) to ensure their adequacy in meeting the legal standards and ISHA's compliance with them. ISHA will ensure that anyone processing personal data on its behalf has received sufficient training to comply with this policy.

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

ISHA will uphold the rights and freedoms conferred by Data Protection Legislation on the individual's whose data it processes and ensure that those rights and freedoms are appropriately taken into account when making decisions which may affect those individuals. ISHA will ensure that it has sufficient controls in place to assist data subjects who wish to exercise their rights.

3.1 Fair, lawful and transparent processing

The processing of all personal data by ISHA will only be undertaken in a fair, lawful and transparent manner, meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the data subject. This will generally, but not always, be via our online privacy notices. All privacy information and any changes to privacy information must be approved by the Data Protection Group (DPG). ISHA's privacy notices can be found on our website.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful ground for the data processing activities intended to be applied to the personal data. The Data Protection Group can provide guidance on lawful grounds for processing. The information process owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control. The lawful basis should be recorded in the relevant department's Data Register. A Data Protection Impact Assessment can be carried out to help establish a lawful basis for a processing activity and the DPG should review and approve this.

Transparency – ISHA will provide information about how personal data is being processed, via privacy notices, to enable sufficient transparency about its handling of personal data. The Data Protection Group is tasked with periodically reviewing transparency and ensuring our privacy notices are accurate and up to date.

3.2 Purpose for processing data

Personal data must only be collected, created or otherwise obtained for specific and legitimate purposes. Our online Privacy Statements and Data Registers list the type of personal data we collect and what we use it for. If you wish to process personal data for a purpose other than which it was originally collected for, you must get the approval of the DPG.

No new data processing activities should be undertaken or commissioned without the approval of the DPG. Senior Managers are responsible for ensuring that all of the data processing activities that they and their teams undertake and/or commission have been approved by the DPG and are recorded in the relevant Data Register.

Special Category Data

Special category data, as defined in the Appendix of this policy, requires additional lawful conditions for processing. When processing any special category data, ISHA must always meet one of the conditions set out in Article 9 of the GDPR.

Personal data concerning someone's race, religion, sex life or sexual orientation will generally only be collected for the purpose of equal opportunity monitoring and should usually be collected with the explicit consent of the data subject. Whereas health data will generally be processed for health and safety requirements, social protection or safeguarding.

3.3 Data minimisation

ISHA will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that it collects. Senior Managers are responsible for ensuring that they and their teams do not collect or create un-necessary, irrelevant or unjustifiable personal data. The DPG can provide advice regarding the justification of personal data collected or created.

3.4 Data quality

ISHA recognises that the accuracy of data it processes is important and that some data is more important to keep up-to-date than others. We will take reasonable steps to keep data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date. Senior Managers are responsible for ensuring that personal data that they and their team have collected or created is maintained, accurate and up-to- date. Personal data which cannot reasonably be assumed to be accurate and up-to-date should be erased or anonymised.

3.5 Data retention and disposal

ISHA will ensure that it does not retain personal data for any longer than is necessary for the purposes for which it was collected. We will delete or anonymise any data when it no longer becomes required for its original purpose. Departmental Data Register owners (senior managers) will be responsible for determining the retention period for the personal data they hold and process in line with ISHA's retention guidelines. The retention period must be recorded in the relevant Data Register. The DPG will periodically review the retention guidelines in line with best practice.

Senior Managers responsible for the relevant Data Registers must review personal data on a continuous basis and ensure that any data that is no longer required is securely anonymised or deleted, as per the Retention Schedule.

3.6 Departmental Data Registers

ISHA maintains Departmental Data Registers as part of its approach to address risks and opportunities involving personal data. ISHA's Departmental Data Registers include the following:
- Business areas that use personal data and the data owner;
- The type of data held;
- The purposes for which the personal data is used;
- Who has access to the data and where it is stored;
- Third party processors or joint controllers
- The retention period and methods of disposal.

3.7 Information and data security

ISHA will ensure that it processes personal data in a secure way, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, and has a separate IT Usage Policy to govern this.

All ISHA staff must ensure that any personal data for which they are responsible, is kept securely and is not disclosed to any third party unless they have been specifically authorised to receive that information and, where relevant, has entered into a Data Sharing Agreement or Data Processing Agreement with ISHA.

Personal data must only be accessible to those who need to use it for work purposes.

Digital personal data
Digitally held personal data must be stored securely, in compliance with the IT Usage Policy. Digital personal data must be:

- Password protected; and/or
- Stored on equipment or devices which are encrypted.

All employees must comply with IT Usage Policy and have read it as part of their induction.

Paper-based personal data
Physical, paper-based personal data must be kept in areas with controlled access or a locked drawer or filing cabinet.

Paper records must be not left where they can be accessed by unauthorised personnel and should not be removed from business premises unless absolutely necessary.

Any staff removing paper records from the office must ensure that they are kept secure, on their person, and that they are carefully stored away to avoid loss or accidental disclosure.

Once paper records are no longer required for their original purpose, they must be destroyed in a confidential manner (e.g. via confidential waste or shredder).

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

3.8 Clear desk approach

To embed many of the principles outlined in 3.7, ISHA operates a clear desk policy approach. When working in the office, or at home, all personal data should be securely stored (whether digitally or physically) when staff are away from their workstation, including locking desktop screens when away for short periods. Office desks must always be cleared at the end of each working day. Clear desk sweeps will be undertaken on an ad hoc basis to enforce this principle.

Staff are responsible for ensuring any personal data that they print is collected promptly and they should only print sensitive personal data and information when absolutely necessary.

3.9 Data subject rights

Data subjects, including our customers and employees, can make a number of information right requests. ISHA will ensure that policies and procedures are maintained so that we are able to recognise such requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about ISHA's processing of personal data and the right to a judicial remedy and compensation

The DPG shall maintain a procedure setting out how information rights requests are to be handled and ensure that the relevant staff are made aware of it.

ISHA will not always be able to exercise an individual's information rights if this would prevent us from carrying out our duties as a social housing provider. For example, a tenant may not be able to exercise their right to be forgotten if they wish to remain in their ISHA home, as there is certain information we have to hold on an individual if we are to be able to provide them with housing. Any complaints in regard to personal data will be handled in accordance with our Complaints Policy via our usual complaints process.

Note: The Freedom of Information Act 2000 does not apply to Islington and Shoreditch Housing Association as we are not designated as a public authority within the terms of that Act. This means that we are not obliged to provide information if we receive "Freedom of Information" requests, but we can provide information voluntarily if appropriate.

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

3.10 Consent

ISHA will interpret consent as defined in the definitions and by law. Consent shall not be valid unless:

•There is a genuine choice of whether or not to consent;
•It has been explicitly and freely given. This must be via opting in, rather than opting out;
•The consent was given by a clear affirmative action undertaken by the data subject;
•ISHA can demonstrate that the data subject has been fully informed about the data processing to which they have consented; and
•Data subjects are clearly able to withdraw consent as easily as it was given and they have been informed about how to do so.

3.11 Personal Data Breaches

ISHA maintains a **Data Breach Reporting Procedure** and will ensure that all employees and those with access to personal data are aware of it. All employees and individuals with access to personal data must report all personal data breaches to the DPG at **dataprotection@isha.co.uk**, who will log and investigate each incident without undue delay.

Appropriate remedial action must be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses should also be reported, recorded and investigated in the same manner. The data breach reporting procedure sets out responsibilities, decision-making criteria and timescales for notifying relevant data subjects and the Information Commissioner about a personal data breach.

3.12 Third Party Data Processors

ISHA reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. Third party data processors must be able to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. Any staff wishing to appoint a data processor must ensure that our procurement procedures are followed and that appropriate due diligence is undertaken on the proposed data processor. The Data Protection Group can provide advice and guidance with this.

A written agreement should be implemented between ISHA and data processors which at least meets the requirements of the Data Protection Legislation. The Governance Manager will ensure that a register of data processing agreements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the contract or data processing agreement.

3.13 ISHA as a Data Processor

Where the organisation acts as a data processor it shall ensure it retains records of processing activities which record at least the information required under Article 30(2) of the GDPR for each controller it acts on behalf of. The organisation shall ensure that it has an appropriate agreement in place with each data controller and shall ensure that its employees, volunteers, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

The Data Protection Group shall implement measures to ensure that this policy is complied with.

3.14 Data sharing, disclosure and transfer

ISHA will only share personal data with third parties where there is a legal basis for doing so and it is necessary for specified purposes. We will ensure that personal data is not disclosed to unauthorised third parties, which could include friends, family members or even the Police. All employees must exercise caution when asked to disclose any personal data to a third party. All ISHA staff will receive training that enables them to deal effectively with such risks.

Generally ISHA will only share personal data where a written agreement is in place covering how the data should be processed and ensuring compliance with data protection legislation. This might be through a contract or data sharing/data processing agreement. Data Sharing/Processing Agreements must be approved by the DPG and the Governance Manager will maintain a register of all such agreements.

Employees are required to use only methods of data transfer approved by the IT Team when transferring digital data externally. Disciplinary action may be taken against employees who fail to observe the IT Usage Policy and use unsafe and insecure methods of data transfer. A proportional approach should be taken in urgent cases.

Urgent and Ad Hoc Transfers
We will take a proportionate approach and urgent or ad hoc data sharing can take place without a written agreement, but only where there is a legitimate and compliant reason for doing so. For example, where information is required by another organisation to investigate a crime (such as CCTV footage), if someone required urgent medical attention, or to help protect a vulnerable person.

3.15 International data transfers

Generally, all data processing and data sharing must take place within the United Kingdom. All of ISHA's servers are based in the United Kingdom. Staff are not allowed to work outside of the United Kingdom or access their ISHA accounts from outside of the United Kingdom.

Any transfer or processing of personal data outside of the United Kingdom may only take place if it is in accordance with one of the exceptions set out in the Data Protection Legislation. The Data

Protection Group should be consulted when data transfers outside of the United Kingdom is being considered.

3.16 Data Protection Impact assessments

ISHA will undertake Data Protection Impact Assessments (DPIAs) whenever there is a possibility that the privacy rights of data subjects may be impacted by the way that we intend to process personal data.

ISHA has a **Data Protection Impact Assessment (DPIA) Procedure** which contains detailed guidance on how and when to carry-out a DPIA. Staff must conduct a DPIA and complete the DPIA form whenever they are:

- Developing or procuring any novel technologies or systems that handle or collect Personally Identifiable Information
- Creating a new program, system, technology, or information collection that may have privacy implications or involve processing a large amount of personal data
- Updating a system that results in new privacy risks
- Updating current or introducing new processes that may change the way in which Personal Identifiable Information is processed

DPIAs help ISHA to anticipate and address the likely privacy impacts of projects, and to ensure that any risks to privacy that arise are addressed appropriately. They must be carried out at the start of the project wherever possible, to allow for problems to be found and addressed during the early stages of the project.

The Data Protection Group will have oversight over DPIAs and must sign them off before the start of the project. ISHA will maintain a register of Data Protection Impact Assessments and the Governance Manager will have ultimate responsibility for this register.

If a DPIA results in a change to the way in which we process personal data, we will update our Privacy Notices to ensure that data subjects are informed of such changes.

3.17 Recording Risk

The DPG will review data protection risks quarterly. ISHA's Governance Manager is responsible for ensuring that any potential data protection risks to the organisation are recorded in the organisation's operational risk register which is regularly reviewed by the Leadership Team. The Leadership Team is responsible for elevating any highly rated risks to the Strategic Risk Register reviewed by the Board.

3.18 Children's data

Special measures will be taken by ISHA if it processes personal data relating to children under the age of 13. We must seek consent from a child's parent or guardian, unless we are making a safeguarding referral, when processing a child's data for reasons beyond our core duty as a landlord.

3.19 Personal data relating to criminal convictions and offences

If the organisation is processing personal data relating to criminal convictions and offences, it shall implement suitable measures, including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

3.20 Training and awareness

ISHA will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in their data protection responsibilities.

All ISHA staff will receive data protection training in the form of e-learning at induction and must complete an assessment so that they are able to demonstrate an understanding of Data Protection compliance. Refresher training will be provided to all staff annually. Managers shall determine if additional training is required for their direct reports and that that training is provided and recorded.

ISHA will raise awareness across the organisation around data protection to keep data protection front of mind through internal communications. Training and awareness raising activities will be logged by the People & Culture manager.

3.21 Record keeping and accountability

In order to fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation as well as in support of transparency and accountability, the organisation will maintain records of the processing activities that it controls, undertakes or otherwise commissions ("RoPAs") as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR. RoPAs at ISHA are its Departmental Data Registers.

The Data Protection Group shall be responsible for ensuring that the Departmental Data Registers are up to date and providing them to the Information Commissioner's Office on demand as required.

3.22 Audit and compliance checking

ISHA will undertake periodic compliance checks, including internal audits by a third party, to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures and action will be taken when failures are found. Records will be kept of all such audits.

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

The Audit & Risk Committee will be provided with a summary of audit findings as and when they take place.

4. ROLES & RESPONSIBILITIES

In March 2018, ISHA's Board determined that it is not required to designate a Data Protection Officer and has documented the rationale underpinning its decision which it shall keep under periodic review.

Data Controller

Islington and Shoreditch Housing Association Limited (ISHA) is the legal data controller under the Data Protection Legislation.

Chief Executive

The Chief Executive of ISHA has overall responsibility for Data Protection and the Data Protection Group.

Executive Directors (Leadership Team)

The Leadership Team is responsible for making sure that sufficient and appropriate resources are available to ensure that ISHA meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

Data Protection Group

The Data Protection Group (DPG) is a working group accountable to the Chief Executive and Leadership Team. The role of the group is to provide review and oversight of data protection and information security matters. Members shall act as ambassadors for ISHA in data protection and information security matters and take a lead in raising awareness in their areas of the business. The DPG has a Terms of Reference outlining the specific responsibilities of the group, with any changes to its remit being approved by the Leadership Team.

The DPG are responsible for the policies, guidance and training needed to ensure ISHA is compliant with Data Protection Legislation. They will monitor and report to the senior management in respect of compliance with this policy, investigate any breaches, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The DPG can be contacted by emailing dataprotection@isha.co.uk.

Senior Managers (Management Team)

Senior Managers are responsible for ensuring that all data processing operations under their sphere of responsibility are undertaken in compliance with this policy and other relevant data protection policies or procedures. They are responsible for:

- reviewing and keeping their Data Registers accurate and up to date, including adherence to data retention guidelines

- ensuring that any Data Processing Impact Assessments required for new projects in their departments are undertaken
- ensuring that relevant Data Sharing Agreements or Data Processing Agreements are in place for their departments and recorded in the register
- ensuring that anyone processing personal data in their teams is sufficiently aware of how this policy applies to their job role and is sufficiently trained to carry out their duties in compliance with this policy.

All staff

Anyone who is directly engaged by the organisation to undertake data processing activities including but not limited to employees, volunteers, casual/temporary/agency workers, directors and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact their line manager or the Data Protection Group. Individuals must complete appropriate training as and when necessary. This will include mandatory online training for all new starters and refresher training for all existing staff. New starters will be required to read this policy and confirm that they have understood it.

Everyone within ISHA has a duty to respect data subjects' rights to confidentiality. Disciplinary action may be taken against staff for non-compliance with relevant policies and legislation.

Partner & Third-Party Responsibilities

Any third party organisations working with or for ISHA that have access to ISHA related personal data, are expected to comply with all relevant data protection legislation. In most cases this will require a Data Sharing or Data Processing Agreement. See Sections 3.12 and 3.13.

5. PERFORMANCE MONITORING

In order to monitor our performance in regard to data protection compliance, key measures will be reported to the Leadership Team and Audit & Risk Committee on a regular basis, unless there is no data to report:

Performance Measure	Regularity of Reporting	Target (where relevant)
Number of data breaches and incidents per month and details on any reported to ICO	Quarterly	Maximum 2 per month
Number of Subject Access Requests (SARs) received per month	Quarterly	N/A – out of our control
Average time taken to complete SARs per month	Quarterly	30 days maximum

An update on any relevant cyber or information security related activities and physical security measures will be presented to the Audit & Risk Committee annually at a minimum.

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

6. REVIEW

This policy will be reviewed by the Board every three years.

7. EQUALITY & DIVERSITY

We do not consider this policy to disproportionately impact any individuals in regard to protected characteristics.

8. ASSOCIATED DOCUMENTS

Policies

1. IT Usage Policy
2. Information & Data Management Policy

Procedures

1. Personal Data Breach Reporting Procedure
2. Subject Access Request Procedures
3. DPIA Procedure

Privacy Notices

Customer privacy notices

a. Tenants
b. Share Owners/Leaseholders
c. Commercial customers

Staff and board/committee members privacy notices

a. Applicants
b. Current staff/board/committee members

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

APPENDIX - DEFINITIONS

Data Controller- defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor-a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller.

Data subject-any living individual who is the subject of personal data held by an organisation.

Personal data - any information relating to a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special Categories of Personal Data - any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Information Asset – data or other knowledge that has value to an organisation

Information Incident- an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information.

Information Security Event – an occurrence in a service, system or network that indicates a possible breach of information security. This includes breaks in policy, failure of controls, or other previously unknown situations.

Personal Data Breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Risk - the chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Reference	Version	Created	Author	Review	Board Approved
Data Protection Policy	3	June 2024	Governance Manager & Company Secretary	June 2027	12 June 2024

Risk Management - the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

RoPA – records of processing activities as required by Article 30 of the GDPR

Corporate Data - any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures.

Recipient -a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Profiling - any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Consent -any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child -under the data protection legislation anyone under the age of 13 is considered a child. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. ISHA shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.