Information Governance Policy

1 Introduction

1.1 Information Governance (IG) is the term used to describe the principles, processes, legal and ethical responsibilities for managing and handling information.

1.2 Stockport Homes Group (SHG) has an obligation to ensure that information is handled legally, securely, efficiently and effectively. The Information Governance Policy sets out the IG Framework: the guidelines and processes that ensure compliance with legislation and best practice. The policy also outlines the relationship with Stockport Council, in relation to the services delivered on their behalf, via the Management Agreement.

2 Context

2.1 This policy details how the organisation will comply with the following:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000
- Environmental Impact Regulations 2004
- Law Enforcement Directive 2016 [(EU) 2016/680]
- Privacy and Electronic Communications Regulation 2003.

2.2 In order to operate efficiently and deliver services effectively, SHG must collect, process and store personal data. This includes information about, but is not limited to:

- Current, former or prospective customers
- Current, former or prospective employees / Board Members / volunteers
- Clients, contractors, consultants and suppliers
- Members of the public.

3 Roles and Responsibilities

3.1 SHG companies are registered with the Information Commissioner's Office (ICO)[1]. The registration numbers are:

- Z9540790 for Stockport Homes Limited
- ZA277767 for Three Sixty (the trading subsidiary of SHG)
- ZA509053 for SKylight
- ZB070553 for Viaduct Partnerships Ltd

[1] The ICO is the UK's supervisory authority for information governance matters

Relationship with Stockport Council.

3.2 Where personal data being processed is in relation to a service which has been delegated under the Management Agreement with Stockport Council, the work will be carried out under a Joint Data Controller[2] agreement.

3.3 Where a service is being delivered by SHG which is not related to the delegated functions within the Management Agreement, Stockport Homes will be the 'Data Controller'.

3.4 Where SHG procures services from a third party by way of a contract, then the contractor/supplier will be a 'Data Processor' where the processing of personal data takes place. A Data Processing Agreement will be put in place in such circumstances. Data Processors themselves are bound by Data Protection legislation themselves.

Data Protection Officer (DPO)

3.5 The Head of Assurance is the DPO for SHG and is responsible for Information Governance, including the production of policies, procedures and guidance, coordination of information requests and the provision of training and advice to SHG.

3.6 Article 39 UK GDPR mandates the tasks of the DPO as:

- To provide advice to the organisation regarding its obligations under the UK GDPR, DPA and other data protection law
- To monitor the organisations compliance with the UK GDPR, DPA and other data protection law and with SHG policies relating to data protection, including the assignment of responsibilities, raising of awareness and training of colleagues involved in processing operations, and the related audits
- To provide advice on Data Protection Impact Assessments (DPIAs) where requested and monitor their performance
- To cooperate with the relevant supervisory authority, acting as the contact point for all issues relating to processing and consultation or where appropriate for any other matter.

3.7 In the performance of the tasks outlined in 3.6, the DPO must have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

3.8 The Head of Assurance reports directly to the Director of Corporate Services, who is a member of Executive Leadership Team (ELT). If needed, the Head of Assurance has full and uninhibited access to the Chief Executive and the Chair of SHG Board.

[2] A data controller determines the purposes and means of processing personal data whereas a data processor is responsible for processing personal data on behalf of a controller

3.9 SHG's DPO can be contacted via assurance@stockporthomes.org. Stockport Council have their own Data Protection Officer (DPO). They can be contacted via: dpa.officer@stockport.gov.uk.

Senior Leadership Team / Board

3.10 Stockport Homes' Board and ELT have a strategic responsibility to ensure that SHG's processes are compliant with relevant legislation. They are also responsible for dedicating sufficient resources to this area and reviewing the framework on a regular basis to ensure that it remains fit for purpose.

Assistant Directors / Heads of Service / Managers

3.11 All Assistant Directors / Heads of Service and Managers are responsible for ensuring effective processes within their teams to ensure colleagues work in line with legislative requirements, corporate policies and best practice. Local processes must ensure data is kept secure at all times and minimise the risk of unauthorised or unlawful loss or disclosure.

3.12 Managers are responsible for ensuring colleagues within their team understand and uphold their IG responsibilities and data security requirements. This includes ensuring their team members complete SHG's data protection training.

3.13 Managers have a specific responsibility in the starter / mover / leaver process to ensure that colleague's email, system and network access reflects the requirements of the role. Amendments to access must be requested by the manager and reviewed on a regular basis.

3.14 Where contractors, consultants, partners and other third parties are engaged in service delivery, it is essential that managers ensure that appropriate contracts and IG arrangements are fit for purpose, legally compliant and that Data Sharing or Data Processing Agreements are in place, as required.

Colleagues

3.15 All employees of SHG have a responsibility to ensure that all aspects of this policy, and any other applicable policies[3], are upheld at all times. In practice, this will mean that any personal data processed as part of their duties is done so in line with legislation, the details of this policy and any other related guidance.

3.16 Colleagues are not entitled to access information on systems / network locations which is not in line with the requirements of their role.

[3] E.g. ICT / Cyber Security Policies

3.17 Colleagues are required to undertake data protection training when they commence their employment and to refresh this at a maximum of every two years. They must follow policies and procedures, and any unauthorised access or use of data will be dealt with as a misconduct issue and a breach of the employment contract.

3.18 Colleagues are required to escalate any information governance issues that they may become aware of in the course of their duties. This can be done by alerting their Manager / Head of Service.

4 Legislative Context

4.1 The General Data Protection Regulation (UK GDPR) regulates the processing of personal data and special categories of data[4]. The Data Protection Act 2018 deals with processing which is not captured by UK GDPR (for example, relating to immigration, national security and derogations to the ICO). It also transposes the Law Enforcement Directive (2016) into UK law.

4.2 The Data Use and Access Act 2025 introduced several reforms to UK data protection law that are particularly relevant for social housing landlords. This brought about some changes related to legitimate interests, subject access requests as well as complaints about data protection practices.

4.3 Article 5 of UK GDPR sets out six principles which must be followed when processing personal information requiring that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and evidence an active approach to minimising / reducing data held where appropriate
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

[4] See Section 6 for further information and definitions

organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.4 SHG must be able to demonstrate compliance with GDPR principles and have documentation to evidence compliance. Stockport Homes holds a "personal data map"[5] of activities that involve personal data processing: the RoPA (Record of Processing Activities). This is updated on a regular basis. See section 8.18 for more information.

5 Types of Data

Personal Data

5.1 Under UK GDPR the definition of "Personal Data" is:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

5.2 Records held by SHG may contain the following personal data:

- Identification details (such as name, address, national insurance number)
- Personal characteristics (such as age, gender, date of birth)
- Family circumstances (such as marital details, family details and household members / relatives)
- Social circumstances (such as lifestyle information, accommodation details, leisure activities)
- Financial details (such as income, expenditure, bank details, benefits and pensions)
- Other information (such as employment details, qualifications and skills, services being provided, referrals, details of complaints, details of support being provided, accident or incidents or enquiry details).

Special categories of data

5.3 Special categories of data can be defined as:

"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,

[5] Also known as a Record of Processing Activities (ROPA) or an Information Asset Register (IAR).

data concerning health or data concerning a natural person's sex life or sexual orientation".

5.4 Genetic and biometric data have been added into this definition under UK GDPR as new definitions of special categories of personal data.

5.5 When special categories of data are intending to be processed by colleagues, a processing condition under Article 6 and a separate, additional processing condition under Article 9 must be met (see later for information about processing conditions). The conditions do not have to be linked but as special categories of data are more sensitive, they are afforded more protection.

5.6 Examples of where SHG may process special categories of data include:

- Collection of equality and diversity information on an application form
- Collecting information about a health condition when dealing with a tenancy, housing support case, anti-social behaviour case, or an adaptation.

Criminal offence data

5.7 UK GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

5.8 Data relating to criminal offences and convictions is that which consists of offending history (commission or allegation) and allegations and proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5.9 To process personal data about criminal convictions or offences, there must be both a lawful basis and either legal authority or official authority for the processing. Schedule 1 of the Data Protection Act 2018 outlines the circumstances in which criminal data can be legally processed.

6 Collecting Data

6.1 SHG collects a variety of personal data to enable the provision of social housing accommodation and associated services which include, but are not limited to:

- Letting, renting, managing and leasing properties
- Carrying out repairs, maintenance and improvements to homes
- Administering waiting lists for housing
- Administering housing and property grants
- Providing associated welfare services, advice and support
- Maintaining accounts and records of financial transactions

- Supporting and managing employees, agents, and contractors
- Carrying out research and policy development
- Providing services to third parties such as schools and public buildings
- Other activities SHG provides.

6.2 SHG collects personal information using CCTV systems both for itself and on behalf of Stockport Council and other partners.

- CCTV is used to monitor and collect visual images for the purpose of security, safety tenancy enforcement and the prevention and detection of crime.
- CCTV systems are operated from a secured control room and there are policies and procedures in place for these activities[6].

6.3 Where personal data is collected about customers or colleagues, a processing condition[7] must be met and explained to the individual, i.e. why the information is required and what it will be used for.

- This is known as a Privacy Notice. Privacy Notices fulfil the UK GDPR principle around fairness, lawfulness and transparency. There are a range of ways in which Privacy Notices can be provided. The overarching Privacy Notice is available on the SHG website and is updated periodically as services, and data processing change.

6.4 Data collected is stored on the SHG's IT network (provided under a service contract by Stockport Council) and IT systems (such as the housing management system, repairs system and document management platforms). Colleagues must follow the ICT / Cyber Security Policies[8] to ensure that security is always upheld. Cyber Essentials Plus certification is held.

7 Processing Data

7.1 Under UK GDPR, the definition of processing is as follows:

"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".

7.2 Articles 6 and 9 of UK GDPR set out the conditions for processing (for personal data and special categories of data). At least one of these conditions must be met, unless a relevant exemption applies. The conditions are:

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (contract)

[6] These are available on Huddle (intranet)
[7] See Section 7 of this policy
[8] See Huddle for more information on cyber security

- Processing is necessary for compliance with a legal obligation to which the controller is subject (legal obligation)
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person (vital interests)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (public task)
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (legitimate interests)
- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (consent).

7.3 If the information being collected, recorded and processed relates to special categories of data, then as outlined above, in addition to satisfying at least one of the conditions at Section 7.2, at least one of the following ten conditions must be met also:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, on the basis of EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the

basis of EU or UK law or pursuant to contract with a health professional and subject to the conditions and safeguards

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8 Working Practices

8.1 To ensure that Information Governance is managed effectively, there are working practices required.

Directing information requests to the Assurance Team

8.2 Requests for information made under UK GDPR / DPA / FOI / EIR must be directed to the Assurance Team. Requests do not have to explicitly refer to legislation. Requests can be made either verbally or in writing. The Assurance Team can be contacted by emailing assurance@stockporthomes.org.

8.3 Requests will be acknowledged, logged and given a unique reference number by the Assurance Team. The team will follow the relevant legislation, policies and procedures to ensure that requests are handled compliantly and responded to within statutory timeframes.

8.4 The Assurance Team may need support of colleagues to respond to information/data requests. Colleagues should respond promptly to requests from Assurance Team for information/data, e.g. copies of emails or other documents.

8.5 The Assurance Team will consider and apply relevant exemptions and/or redactions before releasing to the requestor. For more information, please contact assurance@stockporthomes.org.

Clear Desks and Storage / Security of Information

8.6 To ensure personal data is kept secure the following principles must be applied:

- Colleagues entering Cornerstone or other work locations must carry identification and security fob. This must be kept secure at all times

SHG operates a clear desk policy. That means colleagues must not leave anything on desks at the end of a working day. Information, which is personal, sensitive or confidential must be stored in a secure location. Consider if paper records need to be kept or if they can be scanned and stored. Any paper records must be stored in a lockable cabinet / locker. Personal, sensitive or confidential paper that is no longer required must be disposed of via the confidential paper recycling bins provided. Mobile / agile workers working from home and/or sharing desks must be especially conscious of confidentiality and security of information. This policy covers all information which is processed by SHG, regardless of location

- When moving information between offices or work locations, colleagues and managers must ensure adequate arrangements to uphold data security. Electronic records held on work laptops/devices are more secure than paper records. Paper records should only be used if there is no electronic alternative
- Information held on paper must be returned to the office and secured at the first available opportunity. Destruction of paper records must be via the confidential waste bins provided
- Electronic personal data is made secure by using passwords and restricting access to systems, networks and folders. Passwords must be changed periodically to prevent compromise. Passwords should be reviewed as colleagues leave SHG
- Microsoft (MS) Office suite applications used by SHG are designed to assist with data security and confidentiality and should be accessed and used on all work devices regardless of location
- MS SharePoint, or other document management systems, are used to store work documents. Sensitivity and security levels can be set and applied by SHG. Colleagues also have MS OneDrive's. Documents which are to be used by colleagues across the business should be stored in SharePoint / document management systems to ensure they are easily accessible.

Use of Third Parties

8.7 Contractors, clients, consultants, partners or any other third-party organisation working with SHG must:

- Enter into Data Processing / Data Sharing Agreements as appropriate and required
- Ensure that their staff understand and comply with this Policy and have received the necessary training and guidance to adhere to Stockport Homes' requirements and relevant legislation.
- Allow data protection audits to be undertaken by Stockport Homes' colleagues upon request.
- Be able to demonstrate and evidence that their own internal policies and procedures are legally compliant and meet the needs of Stockport Homes.

- Indemnify Stockport Homes, via contract documentation, against any prosecutions, fines, claims, proceedings, actions, or payments of compensation or damages, without limitation.

8.8 On termination of any Third-Party arrangement, access to SHG systems and/or data should be reviewed and terminated as appropriate.

Multi Agency Working

8.9 It is important that when working in a multi-agency setting, that there is upfront agreement about working practices, data processing and data sharing. This will ensure that IG requirements have been identified from the outset and that agreements have been put in place about how personal data will be processed before the processing commences.

8.10 It may be necessary to complete, or join, a Data Sharing Agreement which sets out the agreed ways in which personal data will be processed in a partnership setting. It will also set out roles and responsibilities on all parties.

Acceptable Use, ICT and Cyber Security and Email Usage

8.11 Acceptable Use is embodied within the relevant SHG IT/Cyber Security Policies. These policies must be adhered to at all times. This is a requirement of the SHG Employee Code of Conduct.

Systems Access

8.15 Colleagues access to data / systems should reflect a need for such access to perform their role efficiently and effectively. Requests for additional or less access should be made and/or approved via the IT portal on Huddle.

8.16 When colleagues move internally between roles, data / systems access should be enabled/revoked by managers as required. Failure to effectively manage data/systems access could result in unauthorised use and/or a data breach.

8.17 Accessing IT systems in a manner which is not consistent with the job role, or a management instruction is gross misconduct and a criminal offence and will be reported to the Information Commissioner's Office (ICO).

Data Mapping / Record of Processing Activity (ROPA)

8.18 SHG keeps a comprehensive record of processing activity that is updated regularly: a 'personal data map' or RoPA.

8.19 The RoPA includes highlights the risks of processing activities alongside mitigating actions. Where risks remain despite mitigation, these will be recorded. The RoPA is a risk register of all personal data processing activities.

Privacy by Design

8.20 SHG's Privacy by Design is approach integrates data protection requirements into all processing activities and business practices, from design

through the entire lifecycle. Opportunities to embed Privacy by Design can be identified by completing a Data Protection Impact Assessment (DPIA), see below.

Data Protection Impact Assessments (DPIAs)

8.21 A Data Protection Impact Assessment (DPIA) is designed to assess a processing activity and determine associated risks. It is required when a processing activity is likely to result in a high risk to the rights and freedoms of individuals. Completing a DPIA will identify risks that have to be considered and mitigated and/or where risks remain and have been accepted with controls in place.

8.22 When a new processing activity is carried out or a new procedure is implemented to existing data processing activities, it may be necessary to consider whether a DPIA is required by assessing the level of risk the new processing activity poses.

8.23 A DPIA will be required if a processing activity on large quantities of data or data that is classed as Special Category (Sensitive) data. It is the responsibility of the relevant department to complete the DPIA, however, support and guidance will be provided by the Assurance Team. The DPO must approve all DPIA's.

9 Right of Access: Subject Access Requests (SARs)

9.1 A data subject[9] has the right to make a verbal or written request to exercise their right of access to their data. This is known as a Subject Access Request or 'SAR'. Requests don't have to explicitly refer to legislation. The key is that the request is clear and demonstrates the individual is seeking their own personal data. Requests can be made either verbally or in writing. SARs should be directed to the Assurance Team for co-ordination and response within one month of receipt of the SAR.[10].

9.2 If somebody wishes to make a Subject Access Request online, they can use a dedicated form on the SHG website[11].The form is not compulsory but aims to simplify the process and maximise efficiency by having clarity on the extent of the request from the first point of contact.

9.3 The requestor is entitled to be:

- Informed as to whether any personal data is being processed by SHG
- Given a copy of any personal data held, where possible

[9] A data subject is a living individual whose personal data is being processed, meaning it's collected, stored, used, or shared in some way. They are the "subject" of the data, and this term is central to data protection laws like GDPR.
[10] The time limit should be calculated to start from the day after receipt of the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. If the date (e.g. 31st) does not exist in the next month then work to the last day of that month. E.g. a request received on 30th January will need to be responded to by 28th February.
[11] https://www.stockporthomes.org/about-us/open-and-transparent/access-information/subject-access-request-form/

- Provided with other supplementary information (e.g. information which should be contained within a Privacy Notice). This may include:
  - A description of the personal data
  - Reasons for it being processed
  - If it is shared with others
  - How it was obtained
  - How long it is retained for

9.4 Once SARs are received by the Assurance Team, they will be acknowledged, logged and given a unique reference number the Team will then follow the relevant legislation, policies and procedures to ensure that requests are handled effectively, compliantly and responded to within statutory timeframes.

9.5 SHG has a duty to ensure they verify the identity of the person making the request. Where the person is known to SHG, for example, is a tenant, there may be existing verification of their ID within SHG systems. If there are doubts about the identity of the person making the request, SHG may ask for more information (e.g. passport or driving licence). This to ensure that the requestor is entitled to receive the information and prevent data breach. SHG will only ask for ID reasonably and proportionately and won't request excessive information.

9.6 The period for responding to a SAR begins when SHG receives the additional identification. The Data Use and Access Act provides more clarity around the "stop the clock" function when more information is required from a requestor.

9.7 If additional ID requested is not received within one month, the SAR will be closed and the requestor informed. The requestor will be made aware of their relevant rights and the option to submit a new request.

9.8 The Assurance Team may need support of colleagues to respond to information / data requests. Colleagues should respond promptly to requests from Assurance Team for information/data, e.g. copies of emails or other documents.

9.9 The Assurance Team will consider and apply relevant exemptions and / or redactions before releasing to the requestor. For more information please contact assurance@stockporthomes.org. It may be necessary for colleagues to provide information for such requests, and this must be completed thoroughly and in a timely manner, as coordinated by the Assurance Team. This may include providing information, documents or copies of emails which are the subject of the request. The Assurance Team will consider whether are exemptions apply and whether any redactions should be applied to the data before it is released to the requestor.

10 Right to be Informed: Privacy Notices

10.1 SHG has a Privacy Notice on its website (see Section 6). This outlines how SHG processes data in a fair, lawful and transparent manner.

10.2 The Privacy Notice is kept up to date as SHG and service delivery functions change and evolve. In some instances, data subjects will be provided with a more specific Privacy Notice relating to the processing which is taking place.

11 Other Data Subject Rights

Right to Rectification / Erasure / Restriction of Processing / Data Portability / Object / Automated Decision Making

11.1 Should a Data Subject wish to exercise one of the above rights, their request must be directed to the Assurance Team who will determine if the right exists (as some are not absolute rights).

11.2 If the right exists, the Assurance Team will confirm this to the requestor and explain what will happen next. They will liaise with internal colleagues as required to enact the right.

11.3 If the right does not exist, the Assurance Team will confirm this to the requestor and provide an explanation as to why their request has not been agreed.

11.4 Please see separate policies on Data Subjects Rights for further information.

12 Information Sharing

12.1 Stockport Homes will share information with its specified partners in accordance with its guidance, policies and procedures. Data Protection Act principles govern how information sharing will take place and colleagues must ensure they:

- Justify the purpose of sharing confidential information
- Only identify the Data Subject if necessary
- Provide the minimum amount of information required
- Restrict access on a strictly need-to-know basis
- Always ensure the security of information
- Are aware of their responsibilities
- Understand and comply with the law.

12.2 Where colleagues are requested to share information, they should seek advice from the Assurance Team and/or DPO as needed and ensure written agreements are in place wherever possible.

13 Data Incidents

13.1 A data Incident can be described as “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”.

13.2 Any incidents will be dealt with in line with the Data Incident Procedure. In certain circumstances, the ICO will need to be informed, this will only be carried out by the IG Team and must happen within 72 hours of anyone within SHG first becoming aware of the breach.

13.3 If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, SHG is required to also inform those individuals without undue delay.

13.4 SHG has robust detection, investigation and internal reporting procedures in place as documented in the Data Incident Procedure. These enable decision making to take place quickly in terms of whether the ICO need to be notified, or not.

13.5 An immediate priority is to recover and secure lost data as quickly as possible and prevent any further data losses occurring. Where the breach involves the loss or misuse of IT equipment, the Head of Technology shall be informed immediately.

13.6 Any incidents are coordinated by the Assurance Team, and they must be informed of any cases without undue delay to enable the correct processes to be followed.

14 Stockport Homes’ Role as an Employer

14.1 It is important that new and existing colleagues understand what personal information is held about them and what this is used for. There is a specific Employee Privacy Notice held within the HR system.

14.2 There are processes and procedures in place to ensure that colleagues’ data is held safely and securely, in line with HR policies, and is only processed for specific purposes. Where appropriate, sensitive (special category) personal information will be kept separate from less sensitive information.

14.3 An employee’s manager will only have access to health information, for example, when there is a genuine need to ensure the employee can carry out their job effectively.

Disciplinary / grievance proceedings

14.4 The DPA 2018 states that organisations should not access or use information kept about employees merely because it might have some relevance to a disciplinary or grievance investigation, where access would

either be incompatible with the purpose it was obtained for or be disproportionate to the seriousness of the matter under investigation.

Monitoring at work[12]

14.5 The DPA 2018 sets out principles for gathering and using personal information obtained through monitoring. Where monitoring may have an adverse effect on employees, the monitoring must be justified by its benefits to the employer or others. This can be demonstrated via a Data Protection Impact Assessment (DPIA).

14.7 People are entitled to a level of privacy at work and so where monitoring is taking place, employees will be made aware of this. Such monitoring may include recording of telephone calls for training purposes or the use of vehicle tracking systems. Where this takes place, there will be relevant HR policies in place.

14.8 Information obtained through monitoring will only be used for the purpose for which it was obtained, unless it is in the individual's interest to do so. Monitoring information will be used if it leads to the discovery of a crime or reveals activity that no employer could reasonably be expected to ignore.

15 Recording Meetings

15.1 There may be occasions when customers, partner agencies or colleagues may want to video, or audio record a meeting that takes place. Recordings of meetings can be carried out in Teams. SHG does occasionally receive requests of this nature and is aware that there are sophisticated recording devices readily available which make both overt and covert recording possible. This may be via a mobile phone or other device.

15.2 Formal meetings, hearings and appeals are often minuted which is deemed to be a sufficient record of the meeting. In addition, full written responses are provided to customer and colleagues queries and complaints. Opportunities are always available for these written records to be discussed and challenged by the people who were in attendance, so video or audio recordings are not permitted for these types of meeting.

15.3 Secret recordings are not allowed.

15.4 Anyone who wishes to record a meeting must make a request of the meeting participants to do so. The right of an individual to refuse to be recorded will always be respected. No customer or member of colleagues will have their voice or image recorded against their will.

15.5 If a request to record is approved, the content of the recording may only be used by the person who requested it (as personal / household usage is

[12] Collecting information about employees by keeping them under some form of observation, normally with a view to checking their performance or conduct.

outside of the scope of UK GDPR). It must not be distributed, uploaded to the internet or social media or quoted selectively. Legal action will be taken against misuse, as required.

15.6 In the case of recording being approved, the recording itself will be made by Stockport Homes, and this will be the responsibility of the meeting's organiser. The original recording will be retained by Stockport Homes and a copy supplied to the customer, partner agency or member of colleagues who has requested that the recording is made.

16 Freedom of Information Act 2000

16.1 The Freedom of Information Act (FOIA) is designed to promote a culture of openness and accountability amongst public authorities. This access to information helps the public make such authorities more accountable for their actions. It gives people the right to access recorded information which is held by SHG. As a wholly owned subsidiary of a public authority, SHG will comply with the FOIA.

16.2 There are two ways that recorded information[13] can be accessed. SHG already publishes information about its activities, and this is documented in the publications scheme. Such information is available in both printed format and electronically, via the website. If a request is for a document available under the publication schemes, then it should be provided. In addition to this, requests can be made for information.

16.3 Freedom of Information Requests (FOIs) must be made in writing. The request must include the requestor's real name, a correspondence address and a description of the information requested. The requestor does not need to explain why they are making the request or even mention what type of request it is however, SHG may seek clarification to determine the exact information that is required to determine the type of request

16.4 Not every request will need to be treated formally under the FOIA. It will often be more pragmatic, and provide better customer service, to deal with it as a customer enquiry. For example, if a customer wants to know when a customer involvement meeting is taking place, this request does not need to be treated formally as an FOI. The information can be given as business as usual. Requests of this nature may prompt an updating of the information made publicly available as it may be a sign that SHG hasn't published sufficient information in its publication scheme.

16.5 A request would be treated formally if the requester has made it clear that they expect a response under the FOIA or if the information requested cannot be provided immediately. This will be the case when information has to be collated from different teams across SHG.

[13] This includes printed documents, computer files, letters, emails, photographs and sound / video recordings

16.6 Responding to FOIs does not include creation of information which does not yet exist. Public authorities are not obliged to create information, only to release information held. In responding to a request, information may be drawn from multiple sources, but there is no requirement to create an answer if the information does not already exist in recorded form.

16.7 Stockport Homes must confirm or deny whether the information is held. If exemptions do not apply, the information will be provided in 20 working days[14]. Information will be provided in the most appropriate format, and this may need to be agreed with the requestor in advance of the response being submitted.

16.8 All FOI requests are logged on a register and coordinated by the Assurance Team to ensure the correct applicability of any exemptions and to enable statutory deadlines to be met.

Refusing an FOI Request

16.9 There are situations in which a request may be refused. This includes if the request is a repeat of a previous request from the same person, if the request is deemed to be vexatious, if it would cost too much[15] or take too much time to gather the information or if an exemption applies[16].

16.10 Some exemptions relate to the type of information being requested, others are based on the potential harm that would or would be likely to arise from disclosure. There is also an exemption relating to the DPA.

16.11 The FOIA exists to avoid unnecessary secrecy. The DPA exists to protect people's right to privacy. It is likely therefore that requests will be made under the FOIA which cannot be responded to because, a person's privacy under the DPA, will be compromised.

16.12 Information can be automatically withheld if it falls under an 'absolute' exemption. Most exemptions, however, are not absolute; they are 'qualified' and require a public interest test[17]. Exemptions are detailed in Part II of the FOIA (sections 21 to 44). If confirming that information is or isn't held may be sensitive, it is possible to give a 'neither confirm nor deny' response.

16.13 Section 14 of the FOIA sets out how to deal with vexatious or repeated requests. Vexatious requests can be described as repeated, unreasonable and nuisance requests. Repeated requests mean that the request is identical or substantially similar to a previous request from the same requestor.

16.14 Where a request for information is refused, the organisation will explain the reasons for this and note the relevant exemption that has been applied. If

[14] The time period begins on the first working day after receipt of the request
[15] If the cost of complying with the request would be more than £450 (18 hours at £25 per hour)
[16] An exemption could mean the organisation isn't obliged to confirm or deny if they hold it, as well as allowing the information to be withheld.
[17] Considering the public interest arguments before deciding whether to disclose the information

the requestor does not agree with the decision, they can ask the Director of Corporate Services to review the decision. If the refusal is upheld, the requestor can then contact the ICO.

17 Environmental Information Requests 2004

17.1 The Environmental Information Regulations (EIR) provides public access to environmental information held by public authorities. It encourages proactive publication of environmental information and ensures members of the public can make requests for information that relates to or affects the environment.

17.2 Examples include information about land development, pollution levels, energy production and waste management. Financial information would be classed as environmental information if it related to the cost of redeveloping land, for example. A full definition of environmental information is provided at regulation 2(1) of the EIR, however, the overall categories are listed below:

- The state of the elements of the environment and the interaction among these elements
- Factors affecting or likely to affect elements of the environment [as included in (a)]
- Measures and activities affecting or likely to affect [as included in (a) and (b)] as well as measures or activities designed to protect those elements
- Reports on the implementation of environmental legislation
- Cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c)
- The state of human health and safety

17.3 It does not include information which does not yet exist. Public authorities are not obliged to create information, only to release information held.

17.4 Requests can be made verbally or in writing and must be responded to within 20 working days. Not every enquiry needs to be dealt with formally if it is sensible to deal with that enquiry in the course of normal business duties. A request will be dealt with formally, via the Assurance Team, if the information can not immediately be provided or if the requester makes it clear they want a response under the EIR.

17.5 The EIR state exceptions that allow for the refusal to provide requested information. Some exceptions relate to the category of information, some to the potential harm disclosure could cause. There is also an exception for personal data as this is covered by the DPA.

17.6 Any such requests should be forwarded to the Assurance Team immediately.

18 Internal Controls

1	**Version control** Version number will change every three years or at major review		
	Version No.	**Date**	**Change/s and reasons for change**
	1	August 2025	Review of existing policy

2	**Policy Owner** i.e. Director	Director of Corporate Services/Deputy Chief Executive
	Policy Author/s i.e. Head of Service	Head of Assurance
	Approved by/date	Director of Corporate Services/Deputy Chief Executive – 6th November 2025 - Decision
	Communication	Team Meeting
	Effective Date - the date of sign-off	6th November 2025
	Next Full Review Date i.e. 3 years after effective date, with an annual light touch review	5th November 2028 or sooner should there be legislative / regulatory changes in this area.

3	Regulatory Standards	Please list the Consumer, Governance, Viability standards and outcomes this policy meets
	Standard/s	**Required outcome**
	Legislation	• UK General Data Protection Regulation • Data Protection Act 2018 • Data (Use and Access) Act 2025 • Freedom of Information Act 2000 • Environmental Impact Regulations 2004 • Law Enforcement Directive 2016 [(EU) 2016/680] • Privacy and Electronic Communications Regulation 2003.

4	**Linked policies/strategies**	• Privacy Policy • Data Subject Rights Policy • Information Governance Charging Policy • Records Management Policy • Data Incident Procedure • ICT Security Policy • Acceptable Use Policy • Employee Code of Conduct

5	**Equality, diversity and inclusion**	Describe how different experiences, characteristics, and approaches were considered during the formulation of the policy, e.g. neurodiversity, age, religion, sex/gender, financial/digital inclusion.
		This policy relates to the collection and use of personal data, which can often include sensitive or confidential data. SHG's policies and working practices outline how that data is safely processed. The policy gives an overview of how people can make requests to access either their own information, or corporate information. There are legislative requirements which relate to information requests and SHG has a Vulnerability Policy which it will utilise to ensure fair access to the request process. Customers will be supported to make requests as required or signposted to other organisations which can provide such support and assistance.

6	**Customer/Colleague Voice**	Describe how the customer and/or colleague voice shapes and influences the policy and services
		Customer / colleague voice has not specifically shaped this policy although as noted above, this policy relates to the collection and use of personal data, which can often include sensitive or confidential data. Any feedback received on the policy / working practices will be considered in future policy reviews. There is a customer privacy notice, a colleague privacy notice and a job applicant privacy notice which exist.

7	**Risk management**	This policy helps to mitigate the following risks identified on the Corporate Risk Register
	Corporate Risk 2	Stockport Homes is not adequately prepared for a proactive inspection of the Consumer Standards by the Regulator of Social Housing
	Corporate Risk 3	Stockport Homes does not maintain a strong, positive reputation where stakeholders have trust and confidence in SHG
	Corporate Risk 7	Stockport Homes does not respond to and learn from complaints effectively and does not listen to the customer voice

8	**Performance monitoring**	Please list the relevant government TSMs (Tenant Satisfaction Measures)
		N/A