Stockport Homes Group
One team, transforming lives

INFORMATION GOVERNANCE POLICY

25 May 2018

Assur

Prepared by:	Assurance Manager	EIA Required?	☐
Date effective from:	25/05/2018	EIA Completed?	☐
Policy approved by:	Assistant Chief Executive	Revision number:	1
Review Date:	25/05/2021	Lead officer:	Assurance Manager

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].

1.2 Stockport Homes Group has an obligation to ensure that information is handled:

- Legally
- Securely
- Efficiently
- Effectively

1.3 This Information Governance Policy sets out details the IG Framework in place to ensure that there are guidelines and processes in place to deliver services effectively, whilst at the same time ensuring compliance with relevant legislation and best practice.

1.4 The Policy also outlines the relationship with Stockport Council, in relation to the services delivered on their behalf, via the Management Agreement.

2 BACKGROUND AND CONTEXT

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

- General Data Protection Regulation 2016 [(EU) 2016/679]
- Data Protection Act 2018
- 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, the Group 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

[1] http://caldicott2.dh.gov.uk/2012/05/21/what-is-information-governance/

3 ROLES AND RESPONSIBILITIES

3.1 Stockport Homes is registered with the Information Commissioner's Office (ICO)[2]. The registration number is Z9540790 for Stockport Homes and ZA277767 for Three Sixty (the trading subsidiary of SHG).

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, this work will be carried out under a Joint Data Controller[3] agreement.

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

3.4 Where Stockport Homes 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

3.5 The Assurance Manager is the Data Protection Officer for Stockport Homes and have a responsibility for Information Governance, including the production of policies, procedures and guidance, coordination of information requests and the provision of training and advice to the Group.

3.6 They can be contacted via: assurance@stockporthomes.org

3.7 Stockport Council have appointed their own Data Protection Officer and this is the Information Governance Service Manager.

3.8 They can be contacted via: dpa.officer@stockport.gov.uk

Management Team / Board

3.9 Stockport Homes' Board and Management Team has a strategic responsibility to ensure that Stockport Homes' 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.

Managers

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

[3] 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

3.10 Managers have a responsibility to ensure that there are effective processes in place within their teams to ensure that staff are working in line with legislative requirements, corporate policies and best practice. This means that there must be local processes in place to ensure that data is kept secure at all times and that the risk of unauthorised or unlawful loss or disclosure is minimised.

3.11 It is a manager's responsibility to make sure all staff within their team are aware of the IG responsibilities and data security requirements and that these are upheld at all times. This includes ensuring their team is fully trained in data protection requirements.

3.12 Managers have a specific responsibility in the starter / mover / leaver process to ensure that employee email, system and network accounts are in line with the requirements of the role the employee is undertaking. Any amendments to access will need to be requested by the manager and reviewed on a regular basis.

3.13 In addition where contractors, consultants, partners and other third parties are engaged in service delivery (via a Data Sharing or Data Processing Agreement), it is essential that managers ensure those arrangements are fit for purpose, legally compliant and that a Data Sharing Agreement or Data Processing Agreement is in place, as required.

Staff

3.14 All employees of the Group have a responsibility to ensure that all aspects of this Policy, and any other applicable policies[4], 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.

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

3.16 Staff are required to undertake data protection training when they commence their employment and to refresh this annually. 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.

3.17 Staff 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.

[4] For example ICT / Cyber Security Policies

4 GENERAL DATA PROTECTION REGULATION 2018 AND THE DATA PROTECTION ACT 2018

4.1 The General Data Protection Regulation (GDPR) regulates the processing of personal data and special categories of data[5]. The Data Protection Act 2018 deals with processing which is not captured by 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 Article 5 of GDPR sets out six principles which must be followed when processing personal information. These require that personal data is:

- processed **lawfully, fairly and in a transparent manner** in relation to individuals (lawfulness, fairness and transparency)
- 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 (purpose limitation)
- **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 (data minimisation)
- **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 (accuracy)
- 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 organisational measures** required by the GDPR in order to safeguard the rights and freedoms of individuals (storage limitation)
- 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 (integrity and confidentiality).

[5] See Section 6 for further information and definitions

4.3 Furthermore, the Group must be responsible for and be able to demonstrate its compliance with these principles with documentation in place to evidence compliance (accountability).

4.4 Stockport Homes holds a "personal data map"[6] of activities that take place which involve the processing of personal data and this is updated on a regular basis.

4.5 Furthermore, an Annual Report will be created at the end of each financial year to outline the framework in place and demonstrate how requirements have been met.

5 TYPES OF DATA

Personal Data

5.1 Under 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 the Group 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).

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

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, 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 GDPR as new definitions of special categories of personal data.

5.5 When special categories of data are intending to be processed by staff, 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 the Group may process special categories of data include:

- Collection 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

5.7 Criminal offence data

5.8 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.

5.9 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.

5.10 To process personal data about criminal convictions or offences, there must be both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10 satisfied. Furthermore, Schedule 1 of the Data Protection Act 2018 outlines the circumstances in which criminal data can be legally processed.

5.11 In addition, further information is provided in the Data Protection Act 2018 (Part 3), which implements the EU Law Enforcement Directive.

6 COLLECTING DATA

6.1 Stockport Homes collects a variety of personal data to enable the provision of social housing accommodation and associated services which include:

- 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

6.2 Stockport Homes also collects personal information using CCTV systems to monitor and collect visual images for the purpose of security and the prevention and detection of crime. CCTV systems are operated from a secured control room and there are separate policies and procedures in place for this area[7].

6.3 Where personal data is collected about customers or staff, a processing condition[8] must be met and it must explained to the individual why the information is required and what it will be used for. This aspect is known as a Privacy Notice and fulfils the GDPR principle around fairness, lawfulness and transparency. There are a range of ways in which Privacy Notices are provided to people. The overarching privacy notice is on the SHG website.

6.4 Data that has been collected will be stored on the Group's IT network (which is provided by Stockport Council by way of an SLA) and IT systems (such as EDRMS and Northgate). Staff must ensure that security is upheld at all times and must follow the ICT / Cyber Security Policies[9] and local arrangements such as use of passwords, secure network areas and restricted system access.

7 PROCESSING DATA

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

7.2 "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] These are available on the HOG

[8] See Section 7 of this policy

[9] http://connect.stockport.gov.uk/kb/Documents/IT/cyber%20security%20Infographic.pdf

7.3 Articles 6 and 9 of 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)
- 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).

7.4 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 8.3, 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 a number of working practices which are required to be followed.

Directing information requests to the Assurance Team

8.2 Requests for information made under GDPR / DPA / FOI / EIR (even where the request doesn't make reference to the specific legislation but the substance of the request makes it clear it is such a request) must be directed to the Assurance Team in the first instance.

8.3 Staff can do this by emailing: assurance@stockporthomes.org

8.4 The Assurance Team will then follow the relevant legislation, policies and procedures to ensure that requests are handled effectively, compliantly and are completed within statutory timeframes. The request will be added to a central log of information requests and given a unique reference number.

8.5 It may be necessary for staff to provide information for such requests and this must be completed thoroughly and in a timely manner, as coordinated by the Assurance Team.

Clear desks and security of information

8.6 To ensure personal data is kept secure at all times, the following principles will be embedded and upheld by staff:

- Staff entering the office are required to have a personal fob and keep this secure at all times
- Cornerstone operates a clear desk policy and staff must not leave any items on desks at the end of a working day. Information which is personal, sensitive or confidential in nature should be stored in a secure location. If this is a paper record then it should be in a lockable cabinet / locker (if it is required to be kept).
- Any personal, sensitive or confidential paperwork that is no longer required shall be disposed of via the confidential paper recycling bins in the print areas on each floor of Cornerstone.
- Employees that are mobile workers, working from home or desk share must be especially conscious of confidentiality and security of information. This Policy covers all information which is processed by The Group, regardless of location.
- When moving information between offices or work locations, staff and managers must make sure there are adequate arrangements in place and that reasonable steps have been taken to uphold data security. It is preferable that paper records are not moved around unless essential and no other possible alternative is suitable (e.g. access an electronic record on a secure laptop rather than take paper forms out of the office).
- Information will be returned to the office and secured at the first available opportunity. If destruction is required, this will be via the confidential waste bins at Cornerstone.
- Electronic personal data is made secure by the use of passwords and restricted access to systems and networks / folders. Passwords shall be changed periodically and should not be easily compromised. Passwords shall also be reviewed as staff leave The Group

Use of Third Parties

8.7 Contractors, clients, consultant, partners or any other third party organisation working with Stockport Homes must:

- Enter into a Data Processing / Data Sharing Agreement as required
- Ensure that their staff are fully aware of 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' staff as required.
- 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.

Multi Agency Working

8.8 It is important that when working in a multi-agency setting, that there is an upfront agreement about working practices, data processing and data sharing.

8.9 This is to 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 SMBC IT / Cyber Security Policies, the adherence to which forms part of the employee code of conduct.

8.12 The corporate network and outlook email system are provided by Stockport Council. As such, please see important cyber security information here. This must be adhered to at all times.

Storing Documents

8.13 The Group has a Records Management Policy[10] in place. The storage of documents falls within the scope of data protection legislation as it is "processing" personal data.

8.14 It is important that documents and records are stored appropriately and securely. This may require restricting of access by use of passwords or secure / restricted network access locations.

8.15 Documents should be easy to retrieve and should not be stored in multiple locations as it makes it difficult to identify the current, approved version of a document. This also uses storage space which is not required.

Systems Access

8.16 When staff are provided with access to an IT system, or network area, it is because they require that access to be able to perform the functions of their

[10] https://thehog.stockporthomes.org/Interact/Pages/Content/Document.aspx?id=14348

role. If additional, or less, access is needed, their manager will need to raise an IT ticket for the change (and authorise it).

8.17 When staff move internally between roles, the existing and upcoming manager must discuss system access and revoke any access which is no longer required to perform the new role. Failure to do so will result in an employee potentially having access to systems for which there is not a justifiable need.

8.18 Accessing IT systems in a manner which is not consistent with the job role or a management instruction is not only a gross misconduct issue, it is also a criminal offence (under data protection legislation) and will be reported to the Information Commissioner's Office (ICO) as a staff data breach.

Data Mapping / Record of Processing Activity (ROPA)

8.19 The Group will keep a comprehensive record of processing activity that is undertaken. This will remain up to date and any new processing activities will be incorporated into the "personal data map" or ROPA.

Privacy by Design

8.20 Privacy by design (or data protection by design) means that the Group takes an approach to integrate data protection requirements into all processing activities and business practices, from the design stage right through the lifecycle of operations.

8.21 This may require the completion of a Data Protection Impact Assessment (DPIA) – please contact the Assurance Manager as required.

9 RIGHT OF ACCESS: SUBJECT ACCESS REQUEST

9.1 A data subject has the right to make a verbal or written request to exercise their right of access (subject access request or 'SAR'). These requests are coordinated by the Assurance Team and must be responded to in one month[11].

9.2 Staff may direct customers towards the DPA 2018 Subject Access Request form on the website. A copy of this document can also be accessed in physical form on the staff intranet. It must be remembered that the form is not compulsory when submitting a SAR. The document aims to simplify and maximise efficiency

9.3 When the SAR form is received the staff member shall complete the relevant sections of the document and escalate to the Assurance team

9.4 If there are doubts about the identity of the person making the request then SHG can ask for more information. This is to ensure that a personal data

[11] 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.

breach doesn't happen. However, it is important that this additional information (related to ID) is only requested when necessary to confirm who they are. The key to this is proportionality.

9.5 SHG will let the requestor know as soon as possible that more information is needed from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information (the request will be placed on hold in between).

9.6 Where verification is not be received within 28 calendar days the request shall be closed. The data subject shall be made aware of this via the most appropriate method (letter/email). The correspondence shall make the data subject aware of their relevant rights and the option to submit a new request.

9.7 The data subject is entitled to be:

- Informed as to whether any personal data is being processed by the Group
- Given a copy of any personal data held, where possible
- 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
    - The reasons for it being processed
    - If it is shared with others
    - How it was obtained
    - How long it is retained for

9.8 All requests should be directed to the Assurance Team (assurance@stockporthomes.org) where they will be recorded on a SAR register and coordinated / complied with centrally. Teams that are required to provide information for the request should do so without undue delay.

9.9 The Assurance Team will consider with any exemptions apply or whether any other GDPR / DPA 2018 terms apply. They will also coordinate the release of the information to the requestor.

10 RIGHT TO BE INFORMED: PRIVACY NOTICES

10.1 SHG has a privacy notice available to all on its website (see Section 6) and this outlines how SHG processes data in a fair, lawful and transparent manner.

10.2 This will be kept up to date as the Group 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 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 will need to be directed to the Assurance Team[12] 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 data subject and explain what will happen. They will liaise with internal colleagues and teams as required to enact the right.

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

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 data sharing protocols. The Data Protection Act principles govern how information sharing will take place and staff must ensure they:

- Justify the purpose of sharing confidential information
- Only identify the customer if necessary
- Provide the minimum amount of information required
- Restrict access to a strictly need-to-know basis
- Ensure the security of information at all times
- Are aware of their responsibilities
- Understand and comply with the law

12.2 Where staff are requested to share information, they should seek advice from the Assurance Manager as needed.

13 DATA BREACHES

13.1 A data breach 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".*

[12] Via assurance@stockporthomes.org

13.2 Any breaches will be dealt with in line with the Information Governance Incident Procedure. In certain circumstances, the ICO will need to be informed. This must happen within 72 hours of The Group 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 documents in the Information Governance 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 IT shall be informed immediately.

14 STOCKPORT HOMES' ROLE AS AN EMPLOYER

14.1 It is important that new and existing staff 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 staff 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 A person'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.

14.4 Disciplinary / grievance proceedings

14.5 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.

14.6 Monitoring at work[13]

14.7 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.

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

14.8 Workers 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.

14.9 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 staff may want to video or audio record a meeting that takes place. This may be because other means of recording, such as note taking, are either unavailable to them or considered to be insufficiently reliable for their purposes. The Group does 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 Stockport Homes will not ordinarily permit the recording of meetings. Formal meetings, hearings and appeals are minuted which is deemed to be a sufficient record of the meeting. In addition, full written responses are provided to customer and staff 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 normally necessary.

15.3 The making of secret recordings is not allowed.

15.4 Anyone who wishes to record a meeting must make a request to do so, stating their reasons why a written record is not sufficient. The right of an individual to refuse to be recorded will always be respected. No customer or member of staff will have his or her voice or image recorded against his or her will unless the person making the recording is processing that data purely for domestic purposes.

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 outside of the scope of GDPR). It must not be distributed, uploaded to the internet or social media or quoted selectively.

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 staff 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 the Group. As a wholly owned subsidiary of a public authority, Stockport Homes will comply with the FOIA.

16.2 There are two ways that recorded information[14] can be accessed. The Group already publishes a vast amount of 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 Requests for information must be made in writing, although they do not have to explicitly state they are a Freedom of Information (FOI) request. The request must include the requestor's real name, an address for correspondence and a description of the information requested. The requestor does not need to explain why they are making the request or even mention that it is an FOI request; however, the Group may seek clarification to determine the exact information that is required.

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 normal 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. The information can be given in the course of normal working practices (business as usual) as part of the Group's commitment to excellent customer service and openness. Requests of this nature may prompt an updating of the information made publicly available as it may be a sign that the Group 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 can not be provided immediately. This will be the case when information has to be collated from different teams across the Group.

16.6 The Group only has to provide information that is already available in a reported form. New information does not have to be created or answers found from a member of staff to a question. In responding to a request, information may be drawn from multiple sources, but there is no requirement to create an answer or obtain information from other sources if the information does not already exist in recorded form.

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

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[15]. 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 request are logged on a register.

16.9 Refusing a request

16.10 There are a number of 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[16] or take too much staff time to gather the information or if an exemption applies[17].

16.11 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.

16.12 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 can not be responded to as in doing so, a person's privacy as afforded to them by the DPA, will be compromised.

16.13 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[18]. Exemptions are detailed in Part II of the FOIA (sections 21 to 44). There may be cases where confirming that information is or is not held may be sensitive and in such cases, it is possible to give a 'neither confirm nor deny' response.

16.14 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.

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

[15] The time period begins once the request has been received in writing

[16] If the cost of complying with the request would be more than £450 (18 hours at £25 per hour)

[17] 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.

[18] Considering the public interest arguments before deciding whether to disclose the information

17 ENVIRONMENTAL INFORMATION REGULATIONS 2004

17.1 The Environmental Information Regulations (EIR) provides public access to environmental information held by public authorities. The main aim of the EIR is to contribute to a greater public awareness of environmental matters by providing greater access to information about the environment.

17.2 This is achieved through proactive publication of environmental information and by ensuring members of the public can make requests for such information. The information covered by EIR is that which relates to or affects the environment.

17.3 Examples of such information 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:

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

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

17.5 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.

17.6 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.

18 LINKS TO OTHER POLICIES

18.1 Stockport Homes has a separate Records Management Policy in place. Staff shall familiarise themselves with this as it has clear links to information governance. Managers will ensure that this policy is adhered to on a local level.

18.2 There is an Information Charging Policy for information requests. This sets out when and by how much a requestor will be charged a fee for the release of information.

18.3 There is an IT Strategy and an ICT / Cyber Security Policy (covering Acceptable Use). These set out guidelines for the use of IT within the Group.

18.4 There is a People and OD Strategy and various People and OD policies and procedures which complement this policy.

18.5 These are all available on the HOG.

19 OWNERSHIP, MONITORING AND REVIEW

19.1 This policy will be reviewed every three years to ensure that it remains fit for purpose. However, it will be updated more frequently should new guidance / legislation be published.