Data Protection Policy

1.0 Introduction

1.1 This Policy outlines how we'll:

- Comply with the:
  - General Data Protection Regulation (GDPR)[1]
  - Data Protection Act 2018
  - Article 8 of the Human Rights Act
  - any associated case law.

- Ensure all employees involved in processing personal information understand their responsibilities.

1.2 The aim of the Policy is to assure the people about whom we hold data that we'll process and store their personal information in accordance with the GDPR.

1.3 This Policy applies to:

- All Southern Housing employees (including permanent, temporary, agency, voluntary, work placement, and contract employees)
- Any members of the Governance structure, including Board Members and involved residents, who have access to personal information
- Our Data Processors, contractors, and agents.

1.4 Throughout the Policy: the terms 'you' and 'your' mean employees, data processors and governance members. The terms 'we', 'our' and 'us' mean Southern Housing.

2.0 What is the General Data Protection Regulation?

2.1 The GDPR sets out legal requirements for all organisations processing personal data. The Regulation is designed to give individuals greater control and protection over the use of their personal data.

2.2 Data Protection law is enforced in the UK by the Information Commissioner's Office (ICO). The ICO can impose strong penalties on us if we don't comply with the GDPR, including criminal prosecution, non-criminal enforcement, and audit. The

[1] References to GDPR in this policy mean the UK-GDPR as supplemented and varied by the Data Protection Act 2018

ICO can issue monetary penalties of up to 4% of Southern Housing's annual turnover, or an unlimited fine in a Crown Court.

Failing to comply with our Data Protection Policy and associated procedures could damage our reputation and lead to a loss of trust in our organisation, as well as having a significant adverse financial effect.

3.0 How will we comply with the Principles of the General Data Protection Regulation?

3.1 We'll comply with the six principles of the GDPR by:

1. Processing personal data fairly, lawfully, and in a transparent manner. We'll not process data unless:

    a) we've identified a valid lawful basis for processing under Article 6 of the GDPR, and
    b) in the case of special categories of personal data, we've also identified a special category condition in compliance with Article 9.

    Articles 6 and 9 are available in Appendix One.

2. Obtaining personal data only for one or more specified, explicit, and lawful purposes. We won't process any data in a manner incompatible with this purpose or purposes.

    We'll never deceive or mislead individuals when we collect their personal information. All forms we use to collect data will clearly state:

    - who we are
    - why we are collecting the information
    - how we intend to use the information
    - where the data subject can find our Privacy Notice
    - any other information we feel is useful.

3. Ensuring the personal data we hold is adequate, relevant and limited to what is necessary in relation to the purpose for which the data was collected.

4. Ensuring personal data is accurate and, where necessary, kept up to date. If we are made aware the personal data we hold is inaccurate we will erase or rectify the data within one month.

5. Ensuring personal data is not kept for longer than necessary in relation to the purpose for which the data was collected. We'll securely dispose of any records we no longer need. Employees must refer to our *Document and Data Retention Policy* for guidelines on how long to keep different types of information.

6. Implementing appropriate technical and organisational measures to protect confidentiality, maintain integrity, and ensure availability of our systems and

services and the personal data we process.

3.2 **Accountability Principle**

To demonstrate our commitment to GDPR principles and acknowledge Southern Housing's responsibility to comply, we will:

a) Maintain data protection policies
b) Implement mandatory employees training and maintain a tailored privacy awareness programme across all teams
c) Maintain relevant documentation on processing activities
d) Adopt the principles of data protection by design and data protection by default, including where appropriate:

- data minimisation projects
- the use of anonymisation or pseudoanonymisation
- Data Protection Impact Assessments for all new projects involving personal data.

3.3 We'll provide a Privacy Notice telling data subjects what to expect when we collect their personal information. The Privacy Notice will state the lawful basis for processing and who we'll share data with.

If we make any changes to our notice, we'll immediately publish the changes on our website, via our online portal for residents, in the next newsletter, and via any other appropriate communication channel.

3.4 If there's a change to the type of personal information we collect or the nature of the processing we'll issue a revised Privacy Notice to all residents, as set out in 3.3. We'll explain the changes, the reason for the changes and the lawful basis for processing.

3.5 There are certain exemptions in the GDPR, which means there are times when we don't have to comply with the above principles, or with data subject rights. These are used only in special circumstances. If employees wish to apply a relevant exemption, they must first contact the Data Protection Team or, in their absence, the Director of Legal Services.

3.6 We'll never rent or sell any personal information to third parties.

3.7 Employees, contractors, and members of the Governance structure are not allowed to use personal information for any other purpose than it was obtained, subject to the exemptions in the GDPR, referenced in 3.5 above.

3.8 Before collecting data for a new purpose, employees must consult the Data Protection Team. This is because:

- It may be unlawful to use the data for another purpose

- We may need to amend our ICO notification (it's a criminal offence if this isn't accurate) and/or Privacy Notice
- We may need to inform data subjects and/or gain their consent
- We may need to complete a Data Protection Impact Assessment if the processing is high-risk.

4.0 Useful definitions within the GDPR

4.1 Data Subject

A living individual who is the subject of personal data or can be identified, directly or indirectly from the data. For us this includes past, present, and prospective:

- Employees
- Residents, service users, leaseholders
- Contractors
- Suppliers
- Partners and agents
- Board members
- Members of the public.

4.2 Data

- Information stored electronically, e.g. on a computer, CCTV, backed up files, faxes, videos, instant messaging, email, information on telephone logging systems, video conferencing, photographs or text messages
- Information generated using automated means e.g. credit score or profiling
- Manual information recorded with the intention it will be processed electronically, e.g. file notes made by hand, which will later be input online
- Manual information that is structured and accessible.

4.3 Processing

Carrying out any operation or set of operations on our data, including:

a) Collection, recording, organisation, adaptation, or alteration of the information or data
b) Retrieval, consultation, or use of the information or data
c) Disclosure of the information or data by transmission, dissemination, or otherwise making available, **or**
d) Alignment, combination, blocking, erasure, or destruction of the information or data.

4.4 Personal data

Data relating to an identifiable person, who can be identified either directly or indirectly (i.e. by reference to an identifier, e.g. location data).

It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.5 **Special categories of Personal data**

Data relating to someone's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation.

4.6 **Data Controller**

The organisation that determines the purpose of the processing, i.e. how the personal data will be used. In our case this is Southern Housing.

4.7 **Data Processor**

Any organisation processing data on our behalf, e.g. our contractors.

5.0 What are our responsibilities?

5.1 The Board is ultimately responsible for compliance with the GDPR.

5.2 The Director of Governance and Regulation will be the named DPO registered with the ICO.

5.3 Our Head of Data Protection will:

- Maintain this Policy and any supporting policies and procedures
- Provide data protection guidance and advice to colleagues and residents
- Manage and advise on breaches
- Provide advice to colleagues on Data Protection Impact Assessments when starting new processes or purchasing new software
- Ensure Southern Housing and its subsidiaries have accurate and up to date ICO registrations
- Act as the contact point for the ICO
- Provide mandatory training for all new employees and annual refresher training for existing employees
- Report annually to Board and Audit and Risk Committee on our data protection management.

5.4 Managers are responsible for implementing this Policy and championing data protection within their teams.

5.5 Southern Housing and its subsidiaries will consider disciplinary action (in accordance with our Disciplinary Policy) against employees who fail to:

- Comply with the GDPR – this includes accidentally, knowingly, or recklessly breaching the Act
- Comply with their duty of confidentiality as outlined in the Probity Policy and this Policy
- Comply with our data protection policy and procedures – and any associated policies and procedures.

5.6 All employees have a duty to maintain the security of personal information. Employees must contact the Head of Data Protection if:

- They're aware of a possible data protection breach
- They're concerned about the way data is being used within the organisation.

6.0 Organisational and technical security

6.1 Ensuring we keep the personal data we hold secure is fundamental to data protection law. We hold lots of personal and special categories of personal data. And have a duty to keep it safe.

6.2 We'll follow the organisation and technical security principles set out in the following policies:

- Acceptable Use Policy
- *IT Access Control Policy*
- IT Information Security Policy.

7.0 Individual rights

The GDPR introduces eight rights for individuals:

1. **The right to be informed**

   We'll be open, honest, fair, and transparent with individuals about the use of their personal data. We'll provide a Privacy Notice as set out in section 3.3 and ensure it's drafted in accordance with guidance provided by the ICO.

2. **The right of access: Subject Access Requests**

   All individuals have the legal right to ask us if we're processing their personal information. The requests are called Subject Access Requests (SARs).

   If we receive an SAR, (or a request that could possibly be one), you must inform the Data Protection Team immediately, even if it's a verbal request.

   We'll comply with SARs in accordance with the GDPR by following our procedure in Appendix Two. We'll respond to SARs promptly and in accordance with statutory timescales.

In some circumstances, an exemption will apply, and this will mean that we can refuse to comply with the SAR (see Appendix Two).

3. The right to rectification

Individuals have the right to ask for their personal data to be rectified where it relates to a matter of fact and it's inaccurate or incomplete and the individual can provide evidence to support this. All requests must be passed immediately to the DP Team. We will respond to all requests without undue delay and within one month.

4. The right to erasure

Individuals can request the deletion or removal of personal data where there is no compelling reason for its continued processing. All requests must be passed immediately to the DP Team. We'll consider requests for erasure by following our procedure in Appendix Three.

5. The right to restrict processing

Individuals have a right to 'block' or suppress the processing of personal data. This only applies to Southern Housing:

- If an individual queries the accuracy of their personal data. We will restrict processing until we have verified the accuracy of the personal data.
- If the processing is unlawful and the individual opposes erasure and requests restriction instead
- If we no longer need the personal data but the individual requires the data to establish, exercise, or defend a legal claim
- Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests) and we are considering whether our legitimate grounds override those of the individual.

If we agree with the request to restrict processing of an individual's personal data, we will continue to store the personal data, but not further process it.

If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data unless it is impossible or involves disproportionate effort to do so.

6. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. We'll consider data portability requests by following our procedure in Appendix Four.

7. The right to object

We will notify individuals of their right to object to direct marketing in our Privacy Notice. We will stop processing personal data for direct marketing purposes as soon as we receive an objection and no later than one month.

Individuals also have the right to object to processing based on legitimate interests. In that case, where an individual objects, we must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or
- The processing is for the establishment, exercise, or defence of legal claims.

8. Rights in relation to automated decision making and profiling

We will only profile residents' data to enable us to tailor the support we provide e.g. to assess the likelihood of residents falling into rent arrears.

We will only profile data provided to us directly by the resident and the lawful basis for processing is the performance of a contract (maintaining our tenancy agreement with residents). We will only use the minimum amount of data required.

We will carry out a Data Protection Impact Assessment before starting any new activity involving profiling of data.

Any requests for human intervention or contesting any decision made by automated decision making must be directed to the Data Protection Team. An assessment of the request will be completed within one calendar month of the request being received.

8.0 Consent

8.1 Some of the services provided by Southern Housing will rely on consent, for example resident involvement and social impact.

Where we require consent to provide a service, we'll follow the requirements set out in the GDPR. Consent requests will be explicit, transparent, and for a specific purpose only. We'll ask individuals to positively opt-in and allow individuals the opportunity to withdraw consent at any time without detriment.

9.0 Taking files and papers out the office

9.1 We understand it's sometimes necessary to take files and papers out the office. But taking personal data out of the building is a serious data protection risk and must be avoided. We'll follow our Procedure for taking files out of the office.

10.0 Home working

10.1 This guidance applies to all employees who work from home, either occasionally or as part of their contract.

10.2 Employees must follow the Procedure for taking files and papers out of the office. Employees may only use online remote access to access our central servers.

10.3 Employees must always follow the Acceptable Use Policy.

10.4 Employees must ensure their work cannot be viewed accidentally by others, including family members.

10.5 Employees must follow the Procedure for taking files and papers out of the office in relation to printing and handling paper documents outside of a Southern Housing office.

11.0 Working with Data Processors

11.1 A data processor is an organisation or individual processing data on behalf of a data controller e.g. a contractor.

11.2 We must have contracts in place with our data processors to cover protection of the data we share with them. The contracts will identify:

- The subject matter and duration of the processing
- The nature and purpose of the processing
- The type of personal data and categories of data subject
- The obligations and rights of the controller.

Our contracts include the following compulsory terms:

- Contractors will only act on our written instructions (unless required by law to act without such instructions)
- Contractors will ensure that anyone processing the data (i.e. employees) are subject to a duty of confidence
- The contractor will take appropriate measures to ensure the security of processing
- The contractor will only engage a sub-processor with our prior consent and a written contract
- Contractors will assist us in providing subject access and allowing data subjects to exercise their rights under the GDPR
- Contractors will assist us in meeting our GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- Contractors will delete or return all personal data to us as requested at the end of the contract, and
- Contractors must submit to audits and inspections and provide us with whatever information we need to ensure they are GDPR compliant and tell us immediately if they are asked to do something infringing the GDPR.

11.3 We'll ensure our contracts are sufficient and legally binding. All managers are responsible for ensuring due diligence is exercised in the selection of a data processor as part of the procurement process.

11.4 We will usually only share any personal information with a data processor once a contract is in place although this will not always be possible or appropriate in the circumstances. The Technology Team will ensure we share information securely.

12.0 Disclosing information to other third parties

12.1 There may be occasions where we receive requests to share personal data with a third party with which we don't have an existing relationship. This can involve a one-way disclosure to a third party or a mutual exchange of personal data.

12.2 Generally, the GDPR does not allow us to disclose information to a third party unless:

- The data subject has been informed (for example through our Privacy Notice) or has given us their consent. We'll still ensure the disclosure meets one of the conditions in Article 6, and one of the conditions in Article 9 if the data is special categories of personal data. For the avoidance of doubt, Southern Housing does not necessarily require the data subject's consent to disclose information to a third party.

- A relevant exemption in the GDPR applies. For example, if the police need information to prevent or detect crime, or catch or prosecute a suspect.

- We believe sharing the information is in the vital interests of the data subject. This is generally life and death situations only and will be rarely used. In these cases we'll also refer to our Safeguarding Adults Policy or Safeguarding Children and Young People Policy.

12.3 As a general rule, we'll not disclose information in response to a telephone request from a third party.

We'll always ensure requests for information are received in writing. Requests must be on letter-headed paper or sent from a legitimate email address. We may verify the identity of the requestor, for example by contacting their organisation.

We'll always respond to requests in writing.

12.4 We'll not disclose information to a third party who visits one of our offices without prior arrangement.

If the request is urgent (for example police visit our office reception) employees must contact the Data Protection Team.

12.5 We'll ensure the third party agrees to return, or securely destroy the information we send when they no longer need it.

12.6 If employees wish to share data with a new third party (who we haven't shared data with before) and:

- We haven't previously notified the data subject
- A relevant exemption doesn't apply,

they must contact the Data Protection Team before sharing data with a new third party. The Data Protection Team will decide if the disclosure is appropriate and record the decision in writing. Even it is a valid request, we will consider whether there is a more appropriate source of the information. We'll only share the minimum amount of information required.

12.7 Residents may authorise third parties to contact us on their behalf, using our form.

12.8 Where a resident is unable to manage their own affairs due to mental or physical incapacity, they may appoint a third person to support, represent, or make decisions on their behalf.

Example 1: For the purpose of managing benefit payments an 'appointee' is treated as though they were the claimant and disclosure is not an issue.

Example 2: In supporting people with dementia, carers may obtain a deputyship certificate or registered power of attorney document. This allows them to access confidential information about the individual.

We'll request evidence of the appointment, and this will be held on the resident's file.

In these instances, we may disclose relevant personal information after verifying the identity of the third party.

13.0 Information Sharing Agreements

13.1 When we engage in regular sharing arrangements with a third party, we'll ensure to the best of our ability that both parties sign an Information Sharing Agreement. These ensure we share certain routine information legally. Before sharing any information under an Information Sharing Agreement, we'll:

- Ensure the agreement covers the type of information we want to disclose
- Follow the specific procedure or authorisation process (outlined in the Governance Framework and Delegations) to ensure we share data fairly and lawfully.

14.0 Using Personal information in corporate publications or on our website

14.1 We'll always obtain explicit signed consent from the data subject before we publish any Personal information. This includes photos taken at corporate events.

15.0 Data Protection breaches

15.1 In the event of a data protection breach, employees must refer to our *Data Protection Breach Procedure*.

15.2 All employees are responsible for reporting data protection breaches to the Data Protection Team immediately if possible and in any event, within 12 hours.

16.0 Information relating to people who have died

16.1 Although the GDPR only applies to living individuals, we will apply the same level of confidentiality to a deceased person's information as we would to a living person's information.

If you ever receive a request for information relating to a person who has died, please contact the Data Protection Team. In many cases it would only be appropriate to release information to the deceased person's executor to their will, or personal representatives (usually their next of kin). We will only share necessary and relevant information.

17.0 Data Protection Impact Assessments (DPIAs)

17.1 We'll consider the potential impact of new initiatives and change on individual privacy and adopt a privacy by design and default approach.

New initiatives which will involve the use of personal data will require a Data Protection Impact Assessment, this will include:

- New or significant change to IT systems storing personal data
- Any changes to how we share or manage personal data e.g. a new surveillance system
- Policy reviews resulting in new ways of managing personal data.

Employees responsible for managing the project/change must complete a DPIA on SharePoint before the project starts. The Governance Team will review the completed DPIA.

18.0 Confirming identity of telephone callers

18.1 All customer facing teams must follow the Procedure for confirming identity of telephone callers.

Each team will have slightly different needs for questions and can choose the most suitable. Questions must be things where there is a strong likelihood only the Data Subject will know the answer. Any change to the agreed security questions must be approved by the Data Protection Team.

19.0 Recording external meetings

19.1 Employees should decline and/or not initiate any request for recordings of external Southern Housing meetings where personal information will, or is likely to be, disclosed. The reasons for this include:

- Protection of privacy for others
- Confidentiality
- To avoid having to manage and store recordings
- To ensure participants feel comfortable contributing to meetings and not limited because of being recorded (or not participate at all).

19.2 In a circumstance where a record and/or transcript are needed as reasonable adjustments, the meeting host will contact the Data Protection Team to discuss how to implement these adjustments.

19.3 If an individual records a meeting and publishes the recording, you should notify the Data Protection Team as they may be subject to charges under the Data Protection Act.

20.0 Recording internal business meetings

20.1 Employees may record internal formal business meetings (e.g Board/Committee meetings) if there's a limited, identified need (e.g. for minute-taking purposes). The organiser of the meeting must communicate with attendees ahead of the meeting to confirm they agree with the recording.

20.2 Any concerns must be addressed directly with the individual and we must ensure colleagues are not excluded from participating if they've concerns about recording.

20.3 At the start of the meeting, the Chair/lead person must explicitly state the meeting is being recorded and the purpose for the recording, and confirm the recording will be stored and deleted in accordance with Southern Housing's procedures.

20.4 The individual recording the meeting must confirm they will not broadcast the recording, post it on social media, or use it for any other purpose than that agreed.

20.5 Recordings must be retained securely on Southern Housing systems with access restricted to colleagues using the recording. The recording should only be retained for the limited time needed to fulfil the original purpose (e.g. to type up minutes). The organiser of the meeting is responsible for ensuring it is deleted from the system.

21.0 Recording internal meetings between colleagues

21.1 With the exception of formal business meetings set out in section 20, it's not permissible to record any other internal meetings between colleagues either in person or virtually using a mobile recording device or meeting app. Examples include but are not limited to team meetings, 121s, appraisals or informal conversations. Meetings recorded without the knowledge or permission of those

present may be treated as grounds for disciplinary action. Employees should refer to the Disciplinary Policy for further details.

22.0 Review

22.1 We'll review this Policy every two years to include legislative, regulatory, best practice development or to address operational issues.

Policy controls

Effective from	16 December 2022
Approved by	Designate Executive Team
Approval date	16 November 2022
Policy owner	Director of Governance & Regulation
Policy author	Jo Mackness - Head of Data Protection (Optivo)

Version history			
Version no.	**Date**	**Summary of change**	**Author and approver**
1.0	16.12.22	New policy	Jo Mackness - Head of Data Protection (Optivo) Designate Executive Team
1.1	12.04.24	22.1 – added we'll review this Policy every two years	Head of Governance & Regulation Director of Governance & Regulation

Appendix One: Lawful Basis for Processing – Articles 6 and 9

When we process personal data, we must meet certain conditions set out in the GDPR. When we process:

- **Personal Data**, we must meet one condition in Article 6 of the GDPR.
- **Sensitive (special categories) of Personal Data**, we must meet one condition in Article 6, and one condition in Article 9 of the GDPR.

Article 6

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Article 9

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

(b) 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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

(c) 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.

(d) 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.

(e) Processing relates to personal data which are manifestly made public by the data subject.

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) Processing is necessary for reasons of substantial public interest, on the basis of 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.

(h) 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 Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

(i) 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.

(j) 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.

Human Rights Act Article 8

If the information shared is of a private nature (e.g. family life) it must meet one of the following criteria – and it must be necessary and proportionate to share:

- Interests of national security
- Public safety
- Economic well-being of the country
- Prevention of crime and disorder
- Protection of health and morals
- Protection of the freedom and rights of others.

Appendix Two: Procedure for Subject Access Requests

Everyone has the right to see the information Southern Housing holds on them (this includes paper and computer files) – this is called a **Subject Access Request (SAR).**

We encourage individuals to use our SAR form as this provides further information on the process.

There is no charge for this request. We'll provide the information without delay and within statutory timescales.

Before providing the information, we'll check the individual's identity eiher by:

- Completing security questions, or
- Requesting two forms of photocopied identification, as set out in the SAR form.

We'll also confirm how they would like to receive the information (by paper or electronic copy).

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we may:

- Charge a reasonable fee, taking into account the administrative costs of providing the information, or
- Refuse to respond.

Where we refuse to respond to a request, we'll contact the individual within one month explaining our reasons for refusal and their right to complain to the ICO.

We may refuse a Subject Access Request for the following reasons:

- It would identify another individual who has not consented to the disclosure and it is unreasonable to disclose without their consent
- It is legally privileged correspondence e.g. between Southern Housing and its solicitors
- The information is held for:
    - the prevention of the detection of crime; and/or
    - the apprehension or prosecution of offenders; and/or
    - the assessment or collection of any tax or duty or any other imposition of a similar nature where access would be likely to prejudice any of the above matters.
- The information was provided in confidence by a third party e.g. social workers, doctors, solicitors, local councils or the Department for Work and Pensions
- In the opinion of Southern Housing or a health professional it would be likely to cause serious harm to the physical and/or mental health of a resident or another person.

The Governance Team deal with SAR requests for residents.

The People Team deal with SAR requests for employees (former and current).

Appendix Three: Procedure for Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

Residents can make a right to erasure request to the Data Protection Team. If we're able to action the request (in full or partially) we will do this within one calendar month.

We will refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- The exercise or defense of legal claims.

Appendix Four: Procedure for Data Portability Requests

Residents can request a copy of their data in a .csv / excel file from the Data Protection Team if the:

- Legal basis for processing the data is consent or performance of a contract AND
- Processing is carried out using automated means excluding paper files.

We will ask for:

- Two forms of identification
- A description of the data requested.

If we're able to provide the data we will provide the information within one month. We will send the file via email, and we will call the resident to confirm their email address and the password to access the file.

We will not accept data portability files from residents or other housing associations at this time. It's a requirement of the GDPR that the data we hold is accurate and up-to-date. To ensure the data meets our requirements and is not in breach of the GDPR we will obtain data directly from residents in line with our internal sign-up procedures.

If requested, we may transfer the data to other housing associations using our SFTP transfer methods if possible. Requests will be referred to the Technology team.