Data Subject Rights Policy

September 2023

Contents

1. Introduction

1.1 SW9 CH understands the importance of protecting its residents, staff and visitors' data. This policy outlines how SW9 CH will govern the processing of personal data in line with data protection legislation.

1.2 The Data Protection Act 2018 (DPA) implements Regulation 2016/679 (EU), commonly known as the General Data Protection Regulation (GDPR). It applies to personal data **(data that allows any living individual to be identifiable)** that is:

- Held on a computer or any other automated system (including e-mails, documents, data on mobile phones, iPads etc.);
- Held in a relevant filing system (a paper system such as client records system, or a set of files on service users that is organised alphabetically by the name of the person or some other identifier such as case number); or
- Intended to go onto computer or into a relevant filing system.

1.3 The Act provides data subjects with certain rights including: the right to be informed; the right to access; the right to restrict processing; and the right to object. We have detailed each of these rights below whilst detailing the measures we will take to ensure compliant satisfaction of these rights.

2. Aims and objectives

2.1 The Purpose of this policy is to enable SW9 CHto:

- Comply with the General Data Protection Regulation (GDPR) in respect of the personal data it uses
- Give guidance about the rights of data subjects
- Protect Network's tenants, staff and partners through commitment to privacy protection and management of their various rights under the legislation.

3. Definitions

- **"Data"** information that is a) processed by means of equipment operating automatically in response to instructions given for that purpose, b) recorded with the intention that it should be processed by means of such equipment, c) recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

- **"Data subjects"** is an individual who is the subject of Personal data. Data subjects have legal rights in relation to the handling and processing of their Personal data.

- **"Personal data"** is any data which relates to an individual who can be identified a) from that data or, b) from that data and other information in our possession or likely to come into our possession. Personal data can be factual (i.e. name, address or date of birth) or an opinion (e.g. performance appraisal).

- **"Data Controller"** is a person who (either alone or jointly with other persons)

determines the purposes for which, and the manner in which, any Personal data is to be processed. They have a responsibility to establish practices and policies in line with the Act.

- **"Data users"** are all employees whose work involves the use and or processing of Personal data. Data users have a duty to protect the information they handle by following and adhering to the Data Protection and Information Security policies at all times.

- **"Data processors"** is any person, other than an employee of the Data Controller who processes Personal data on behalf of a Data Controller, i.e. third parties that process or handle Personal data on our behalf.

- **"Processing"** is any activity that involves use of Personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasure or destruction. Processing also includes transferring Personal data to third parties.

- **"Sensitive Personal data"** (also referred to as special – categories of data) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal data can only be processed under strict conditions, and usually requires the express consent of the data subject.

4. Roles and Responsibilities

4.1 It is a condition of employment that all employees, contracted third parties and individuals abide by the policies endorsed by SW9 CH.

4.2 Any person, who considers that this policy has not been followed in respect of being able to exercise one of their rights over personal data relating to themselves, or others, is to raise the matter directly with their line manager, or, if the matter cannot be resolved, with the Data Protection Officer or HR.

5. Policy statement

5.1 The scope of this policy applies to all employees and any third party or individual, who conducts work on behalf of SW9 CH.

5.2 SW9 CH will ensure compliance to enabling the various rights of data subjects::

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure

- Right to restrict processing
- Right to objection
- Right to portability
- Right regarding automated decision making and profiling

5.3 A data subject can exercise these rights to any member of SW9 CH staff or acting agent including data processors.

6. Right to be informed

6.1. The right to be informed encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over our uses of personal data.

6.2 The information we will supply relating to the processing of personal data must be:
- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

6.3 The use of data, including how we protect and store data, will be made readily available to individuals through our privacy notice on our website and the below summarises the information we should supply to individuals under Article 13 of the GDPR.

a) The identity of the organisation
b) The purpose(s) for which Personal data will be processed
c) Information regarding the disclosure of Personal data to third parties
d) Information regarding the individuals' right of access to Personal data
e) Whether Personal data is transferred outside the EEA
f) How to contact the Data Protection Officer
g) Details of specific technologies or electronic measure to collect information about individuals, e.g. website cookies.

6.4 In addition to our privacy notice/statement on the website, all forms or document that collect personal data should have a Fair Processing Notice (FPN). A Fair Processing notice is a statement which describes why we are collecting the personal data, what we plan to do with it, what lawful basis we are relying on (and what condition we are relying on if it is special category of personal data), whom it will be shared with, how long we will keep it and a link to the website's data protection pages.

6.5 Data must be supplied at the point of collection of personal data or within fourteen days after receipt of personal data from an external source where the individual is not aware data has been shared with us. If personal data is provided by an external source, the data subject/s should be provided with a Fair Processing Notice email which also confirms whom we received the personal data from.

7. Right of Access

7.1 The right of access, commonly referred to as subject access, gives individuals the

right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their data, and check we are doing it lawfully.

Individuals have the right to obtain the following from us:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that we provide in our privacy statement or fair processing notices on forms.

7.2 An individual can make a subject access request ("SAR") to us verbally or in writing. It can also be made to any part of our organisation (including social media accounts) and does not have to be to a specific person or contact point. We have an optional web form on our website which we encourage the use of, but this is not compulsory. Therefore, should an individual make a request or reference to obtaining their personal data it is expected that staff will take a full note of the request and send to dpo@sw9.org.uk without undue delay.

7.3 Where staff have authority to disclose and access to the data requested, they are expected to action the request without undue delay ensuring any third-party data is redacted. Where there is no access and/or authority to the requested data, staff are required to contact dpo@sw9.org.uk

7.4 Examples of data requests managed by the Business Support Team team:

- If the data subject expressly refers to their rights under data protection law,
- **If they are asking for multiple types of data held around the organisation.**If they are asking for 'all their data' or data for a long period of time (6 years+).

7.5 It is important to note that the request does not have to include the phrase 'subject access request' or 'data protection', as long as it is clear that the individual is asking for their own personal data.

7.6 If an individual makes a request electronically, we will provide the information in a commonly used electronic format via a secure sharing file portal, unless the individual requests otherwise.

7.7 The information should be provided free of charge to the individual except where the request is manifestly unfounded, excessive or requires additional copies. In these circumstances we will rely on an exemption under the legislation to charge a "reasonable fee" for the administrative costs of complying with the request.

7.8 There may be an exemption to providing the data requested that we can rely on. For more information on costs, timeframes and exemptions please refer to the Subject Access Request Procedure.

8. Right to rectification

8.1 Under Article 16 of the GDPR individuals have the right to have inaccurate

personal data rectified. An individual may also be able to have incomplete personal data completed although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

8.2 This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although we may have already taken steps to ensure that the personal data was accurate when we obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

8.3 If you receive a request for rectification, you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject with the support of the Data Protection Officer if needed. The right of Restriction should be applied whilst evidence is being considered.

8.4 Should a decision be taken not to amend the data you must notify the Data Protection Officer without undue delay and within one month of receiving the request. This is so they can send a formal response confirming SW9's position on this matter and update the DPO register with the rational that led to the decision for this request.

9. Right to Erasure

9.1 This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller (Network).

9.2 The Right to Erasure is not absolute and will only apply in the following circumstances:

a) The personal data is no longer necessary in relation to the purpose for which it was originally collected
b) The processing was based on consent, and the Data Subject has now withdrawn their consent
c) The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller
d) The data was being unlawfully processed
e) The data must be erased to comply with a legal obligation

9.3 All requests for erasures should be sent to the DPO mailbox, who will send notifications to teams to restrict the processing of that data and carry out a search of our systems for the data held. Please refer to guidance on staff intranet on how this request will be actioned.

9.4 A record of deletion will be kept to enable us to evidence compliance with the data protection legislation. Such record will contain data subjects name and any personal identifiers, date request made, decision taken, date of deletion (if applicable).

10. Right to Restrict processing

10.1 Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar detailed in Articles 18 (Right to restriction of processing) and 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing) respectively.

10.2 When processing is restricted, we are permitted to store the personal data, but not process it further. We can retain just enough information about the individual to ensure that the restriction is respected in future. This needs to be applied and communicated to each data processor where applicable and documented where appropriate.

10.3 We are required to restrict the processing of personal data in the following circumstances:

- Where an individual contest the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data. We would do this by asking the individual to confirm the information is correct and where required update accordingly.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual.
- This can only be confirmed by way of evidenced consent from the individual or for the purpose of criminal proceedings.
- When processing is unlawful and the individual opposes erasure and requests restriction instead, we are obliged to ensure this request is documented and the data collected is only used for the intent on which it was originally collected for, and not process it further.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim. We would ask the individual to submit a SAR and release the data upon receipt and in accordance with the SAR procedure.
- We may need to review procedures to ensure we are able to determine where you may be required to restrict the processing of personal data.
- 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. We must inform individuals when we decide to lift a restriction on processing.

10.4 All requests for restriction should go to the DPO mailbox without undue delay as we only have one calendar month to respond to the request subject to exceptions.

11. Right to Data Portability

11.1 This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format, for example, Excel or CSV file.

11.2 The Right to Data Portability only applies in the following circumstances:
a) When the personal data was provided to the controller directly by the Data Subject
b) Where the processing is based on consent or performance of a contract
c) When processing is carried out by automated means

11.3 All requests for portability should go to the DPO mailbox without undue delay as we only have one calendar month to provide the requested data.

11.4 Any electronic data sharing must be done securely in line with our IT policy.

12. Right to Object

12.1 Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

12.2 The Individual must have an objection on "grounds relating to his or her particular situation".

12.3 If the right to objection is exercised, we must stop processing the personal data unless:
a. We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
b. the processing is for the establishment, exercise or defence of legal claims.

12.4 If we process personal data for direct marketing purposes, we must stop processing personal data as soon as we receive an objection. We have no exemptions or grounds to refuse.

13. Automatic Decision Making and Profiling

13.1 Under the act data subjects have the right to be told about whether we do any automated decisions including algorithms, system filtering or profiling. This right provides safeguards for individuals against the risk that a potentially damaging decision being taken without human intervention. It concerns:
a) automatic decision making (a decision is solely made by automated means and not human involvement) and;
b) profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

13.2 This right applies when the decision is based on automated processing and/or it produces legal/significant effects on the individual. However, this right will not apply if the decision relates to the following circumstances:
a) Is necessary for entering into or performance of a contract
b) Is authorised by law

c) Is based on explicit consent
d) Does not have a legal/significant effect on the data subject

14. Cost and timeframe to carry out the requests and exercise the rights above

14.1 In most cases we will be unable to charge a fee to comply with any of the data subject right request. However, where the request is manifestly unfounded or excessive, we may charge a "reasonable fee" for the administrative costs of complying with the request.

14.2 Unless stipulated differently in related procedure/policy or a statutory exemption applies then the request must be completed within one calendar month from the date of receipt.

14.3 We will calculate the time limit from the day after SW9 received the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond. This means that the exact number of days we have to comply with a request varies, depending on the month in which the request was made.

15. Complying with this policy

15.1 Monitoring compliance - The Data Protection Officer will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and general feedback about business procedures.

15.2 Exceptions - Any exception to the policy must be raised with the Data Protection Officer in advance of exceptions taking place.

15.3 Violations/Non-Compliance - **Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct**. A violation of this Policy as well as any supporting policy documents must be treated as an incident and investigated, the findings of which will be handled in accordance with Network's disciplinary procedures, and could lead to termination of employment, or in the case of third parties, termination of the contractual relationship with the company; in certain circumstances this could give rise to legal proceedings.

16. Legislation and regulation

16.1 The legislation listed in this policy is not intended to cover all legislation applicable to this policy. To meet the required HCA outcome on adherence to all relevant law, Network will take reasonable measures to ensure compliance with any and all applicable legislation by reviewing policies and procedures and amending them as appropriate. The legislation listed within this policy was considered at the time

of the development of this policy, but subsequent primary and secondary legislation, case law and regulatory or other requirements will be considered and the policy reviewed and adopted in accordance with the requirements set out therein, even should such subsequent legislation not be explicitly listed within this policy. Any queries relating to the applicable legislation should be directed to the policy author.

17. Equality and diversity

17.1 We will apply this policy consistently and fairly and will not discriminate against anyone based on any relevant characteristics, including those set out in the Equality Act 2010.

18. Review

18.1 All policies should be reviewed every 3 years as a minimum, or sooner if there is a specific legislative, regulatory or service requirement or change in guidance, law or practice.

Policy author:	**Policy and Performance Lead**	
Policy owner:	**Head of Corporate Services**	
Adopted from Network Homes: y/n	**Y**	
Review schedule (1, 2 or 3 years):	**3 years**	
Equality Impact Assessment (EIA)	**Date completed**	
	Initial or full EIA	

Change Record

Date	Reviewed by (name and title)	Version	Summary of changes