Consent Policy

September 2024

Contents **Page**

Appendices

None

1. Introduction

1.1 This policy sets out when consent required for processing data and how consent is to be obtained and recorded.

1.2 Under the Data Protection Act (2018) and the UK GDPR, consent is one of the lawful bases for processing personal data. It is vital that consent is obtained fairly and transparently in order to give residents in control of how their data is used and to minimise the risk to the organisation.

1.3 Consent is only appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. If you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair. If you make 'consent' a precondition of a service, it is unlikely to be the most appropriate lawful basis. Consent is not always required. It is simply one of the lawful bases amongst six available options including:

- For the purposes of contracting with the individual
- Compliance with a legal obligation
- In the vital interests of the data subject
- In the legitimate interest of the business
- In the interests of the public

1.4 You need consent when no other lawful basis applies. Examples are:

- If you want to use or share someone's data in a particularly unexpected or potentially intrusive way, or in a way that is incompatible with your original purpose.
- If you are using special category data (ethnicity, sexuality, religious beliefs, health data etc.)
- Under E-Privacy laws (Privacy and Electronic Communications Regulation) for marketing calls or messages, website cookies or other online tracking methods, or to install apps or other software on people's devices

2. Aims and objectives

2.1 The purpose of this policy is to enable SW9 to:

- Comply with the law in respect of the personal data it uses
- Follow best practice when obtaining consent
- Ensure consent has been obtained fairly and according to the terms required by the DPA (2018).
- Ensure all consent obtained is valid under DPA Requirements
- Ensure consent is able to be withdrawn as easily as it was given
- Ensure staff are aware of their responsibilities in respect to obtaining consent fairly
- Ensure clear guidance and tools are available to staff to be able to comply

with any updates to data protection legislation.

3. Performance monitoring and responsibilities

3.1 The Data Protection Officer (DPO) is responsible for:

- Ensuring there are controls and procedures in place to support company compliance with current legislation relating to Data Protection
- Ensuring that appropriate controls and procedures are in place to support 'fair processing' statements being made when the company, its agents, contractors or service providers collect or process personal data for which the company is the Data Controller, and that these reflect the purposes for which the information may be used and any other parties to whom the information may be revealed (Principle 1).
- Ensuring there are controls and procedures are in place to support staff to obtain appropriate consent for the personal data they process or store if applicable.
- Ensuring there is a continuous review of consent procedures and this policy when changes occur in legislation or business process.
- Ensuring this policy is communicated to employees as part of their Induction Training Program and that they receive refresher training annually thereafter. A formal record of all training is to be retained against the individuals' personal records.

3.2 Staff with day-to-day responsibilities for processing personal data in any form must be able to demonstrate competence in their understanding of the data protection legislation as well as being able to describe the processes through which this is implemented within the business.

3.3 Third party suppliers that store or process personal data on behalf of the organisation are designated Data Processors and shall be bound by an Information Sharing Agreement or a data sharing clause in the relevant contract.

4. Valid Consent

4.1 Network will ensure that it commits to the standard for consent that is outlined in the DPA (2018). This states that:

- Consent is unambiguous and involves a clear affirmative action
- Consent is separate from other terms and conditions and not a precondition to signing up to a service
- Consent is granular for distinct processing operations , i.e. Consent obtained is specific to each purpose of processing and not applied to a variety of processing with different purposes
- Consent obtained is able to be evidenced
- Consent is obtained as part of a process where clear and transparent communication has taken place

- Consent is obvious and requires a positive action to opt-in
- Consent specifically identifies the controller and the purposes of the processing
- Consent obtained is able to be withdrawn as easily as it was obtained
- Consent obtained is not in conflict with respect to the relationship between the data subject and Network Homes where there could be seen to be an imbalance in power
- Consent procedures are reviewed to ensure they are in alignment with any update in legislation

5. Obtaining Consent

5.1 Process - All consent obtained must specify exactly how the resident's personal data will be used. Consent must be 'explicit' and affirmed in a clear statement (either oral or written) – this means that they cannot be asked to "opt out" with opting in as the default. SW9 will ensure that residents signify agreement via a clear affirmative statement and forms will include detail of the processing that requires consent.

5.2 Information that needs to be included in consent obtaining - SW9's procedures for obtaining consent will include as a minimum the following:

- The name of the organisation and the names of any third parties who will rely on the consent
- The purposes of the process
- The processing activities
- The ability to withdraw consent at any time
- How to withdraw consent once given

5.3 Methods for obtaining consent **–** SW9 will employ some of the following mechanisms when obtaining consent from individuals:

- Signing a consent statement on a paper form;
- Ticking an opt-in box on paper or electronically;
- Clicking an opt-in button or link online;
- Selecting from equally prominent yes/no options;
- Choosing technical settings or preference dashboard settings;
- Responding to an email requesting consent;
- Answering yes to a clear consent request;

5.4 SW9 will not rely on silence, inactivity, pre-ticked boxes, opt-out boxes, default settings or a blanket acceptance of terms and conditions to imply consent. The organisation will seek to adopt user-friendly methods at all times.

5.5 Online consent - When obtaining consent online, it will not be an enforced policy to ensure data subjects create user accounts and sign in just to confirm verifiable consent (although this may be a suitable option). Particularly in the case of cookie

consent, linking the consent to a temporary session ID will be deemed as acceptable.

5.6 Children's consent for online services - If there are any services requested and delivered over the internet to children (other than preventive or counselling services), then parental consent must be obtained for any individuals under the age of 16. SW9 will ensure to implement age-verification measures and make 'reasonable efforts' to verify parental responsibility for those under the relevant age.

6. Recording Consent

6.1 SW9 will ensure there is an effective audit trail of how and when consent was given, so that evidence can be provided if challenged. Records will be kept when consent is obtained in order to demonstrate the following:

- The name of the individual (or other identifier such as user name or session ID) who consented
- When consent was given (a copy of a dated document, or online record that includes a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation)
- What was communicated at the time of consenting (a master copy of the document or data capture form containing the consent statement in use at the time, along with any separate privacy policy, including version numbers and dates matching the date consent was given)
- If consent was given orally, the records should include a copy of the script at the time
- How the individual consented (for written consent, a copy of the statement or data capture form)
- If consent was given online, records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form.
- If consent was given orally, a note of the consent made at the time of the conversation, rather than the full record of the conversation.
- Whether consent has been withdrawn , if so, when.

7. Withdrawal of consent

7.1 SW9 will ensure data subjects are provided with the right to withdraw consent 'at any time' on their own initiative and that withdrawal is as easy as it was to give consent. Withdrawal of consent will apply only when the legal basis for processing was initially based on consent.

7.2 Withdrawal of consent by third parties - Where individuals decide to use a third party acting on their behalf to withdraw consent, SW9 will ensure there are mechanisms in place to verify that the third party has the authority to do so.

8. Consent validity period

8.1 Withdrawal of consent - Consent should not be deemed to be ‘eternal’.Consent expiration will depend on the context of situation in which the context was obtained however consent automatically expires as soon as a data subject withdraws their consent, and any processing which was relying on consent as the legal basis must stop in the absence of an alternative legitimate basis to continue the processing. The data subject must be informed of this if the processing is to continue.

8.2 Processing changes - Network will aim to obtain fresh consent if the purposes for the processing or the activities being carried out in the processing are changed. Consent cannot be deemed to be ‘evolving’ as the process evolves.

8.3 Consent refreshing periods - SW9 will aim to obtain fresh consent every 10 years as a mechanism for best practice and ensuring that it is being fair to individuals and equally not being unnecessarily disruptive to its audience by repeatedly requesting consent.

8.4 Parental Consent - Parental consent will always expire when the child reaches the age at which they can consent for themselves. Consent will then need to be reviewed and fresh consent obtained from the child who is now at an age where they can consent for themselves.

9. Complying with this policy

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

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

9.3 Violations/Non-Compliance - Unauthorised use of Personal data (particularly where consent is applicable), is a disciplinary matter that may be considered a gross misconduct.

9.4 A violation of this Policy as well as any supporting policy documents and Operating Standards 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.

10. Related documents

- Data Protection Compliance Policy
- Consent Management Procedure

11. Legislation and regulation

The legislation listed in this policy is not intended to cover all legislation applicable to this policy. To meet the required RSH Governance & Financial Viability Standard 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.

12. Equality and diversity

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.

13. Review

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.