

GDPR Policy	
Policy Number:	SBP005
Lead Person:	Abbie Cavanagh, Director
Last Review (Date)	28.09.2025
Next Review to commence (Date)	27.09.2026 <i>Earlier review may take place where changes in legislation, guidance, business activities or identified risks make revision necessary.</i>

Contents

1. Introduction
2. Definitions
3. Data protection officer & scope of policy
4. Recruitment data processing overview
5. The data protection principles
6. The rights of data subjects
7. Lawful, fair and transparent data processing
8. Consent
9. Specified, explicit and legitimate purposes
10. Adequate, relevant and limited data processing
11. Accuracy of data and keeping data up to date
12. Data retention
13. Secure processing
14. Accountability and record keeping
15. Data protection impact assessments and privacy by design
16. Keeping data subjects informed
17. Subject access requests
18. Rectification of personal data
19. Erasure of personal data
20. Restriction of personal data processing
21. Data portability
22. Objections to personal data processing
23. Automated decision making and profiling
24. Direct marketing
25. Personal data collected, held and processed systems
26. Transfers of personal data outside the UK
27. Data breach notification
28. Information commissioner's office (ICO)

1. Introduction

This Policy sets out the obligations of SH (North) Ltd, a company registered in the United Kingdom under number 16744681, whose registered office is at 1 Maling Court, Union Street, Newcastle upon Tyne, NE2 1BP ("the Company"), regarding data protection and the rights of individuals in respect of their personal data under UK Data Protection Legislation.

This Policy applies to all personal data processed by the Company in the course of its recruitment business activities, including candidates, clients, employees, contractors, suppliers and other third parties.

This Policy sets out the Company's obligations regarding the collection, processing, transfer, storage and disposal of personal data. All employees, contractors, agents and third parties working on behalf of the Company must comply with this Policy at all times.

2. Definitions

“Consent” means a freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they signify agreement to processing of personal data.

“Data controller” means the organisation which determines the purposes and means of processing personal data. The Company is the data controller of all personal data it processes in the course of its business.

“Data processor” means a person or organisation which processes personal data on behalf of a data controller.

“Data Protection Legislation” means all applicable data protection laws including UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations 2003 (as amended).

“Data subject” means a living identified or identifiable individual.

“Personal data” means any information relating to an identified or identifiable individual.

“Personal data breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

“Processing” means any operation performed on personal data including collection, storage, use, disclosure, alteration or deletion.

“Special category personal data” means sensitive personal data including racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, sexual orientation, biometric and genetic data.

3. Data protection officer & scope of policy

The Company’s Data Protection Officer is the Director, 1 Maling Court, Union Street, Newcastle upon Tyne, NE2 1BP.

The Data Protection Officer is responsible for overseeing compliance with this Policy and ensuring appropriate data protection governance is maintained.

All managers are responsible for ensuring staff comply with this Policy and for implementing appropriate controls, training and operational safeguards.

Any questions relating to data protection should be directed to the Data Protection Officer at abbie@standbyhealthcare.com, 0191 646 0100.

4. Recruitment data processing overview

As a recruitment business, the Company processes personal data for the purpose of introducing candidates to clients for permanent, temporary or contract employment opportunities.

The Company collects and processes the following categories of personal data:

- Identity and contact details
- CVs, employment history and qualifications
- Right to work documentation
- Professional references
- Background check results where applicable
- Payroll and assignment details (where applicable)
- Client contact details and recruitment requirements

Personal data is collected directly from candidates, clients, referees, job boards, professional networking platforms and recruitment databases.

The Company uses applicant tracking systems (ATS), CRM systems, email systems and cloud-based software to manage recruitment activity and candidate matching.

5. The data protection principles

The Company shall ensure that all personal data is:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Retained only for as long as necessary
6. Processed securely using appropriate technical and organisational measures

6. The rights of data subjects

Data subjects have the following rights under UK GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights relating to automated decision making and profiling

7. Lawful, fair and transparent data processing

The Company processes personal data under one or more lawful bases including:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Where legitimate interests are relied upon, the Company ensures a balancing test is carried out to ensure individuals' rights are not overridden.

Special category personal data is only processed where a condition under UK GDPR Article 9 is met.

8. Consent

Where consent is relied upon:

- It must be freely given, specific and informed
- It must be separate from other terms
- It must be capable of being withdrawn at any time
- Withdrawal must be as easy as giving consent
- Records of consent must be retained

Consent is not generally relied upon for core recruitment processing but may be used for marketing or special category data where required.

9. Specified, explicit and legitimate purposes

The Company processes personal data only for recruitment-related purposes including:

- Candidate sourcing and placement
- Matching candidates to job roles
- Client recruitment services
- Payroll and assignment administration
- Compliance with legal obligations
- Maintaining candidate talent pools where appropriate

Individuals are informed of processing purposes at the time data is collected.

10. Adequate, relevant and limited data processing

The Company ensures that only personal data necessary for recruitment purposes is collected and processed.

Employees must not collect excessive or irrelevant personal data.

11. Accuracy of data and keeping data up to date

The Company ensures that personal data is accurate and kept up to date.

Reasonable steps are taken to correct or erase inaccurate data without delay, including updates requested by data subjects.

12. Data retention

Personal data is retained only for as long as necessary for recruitment and business purposes.

Typical retention periods include:

- Unsuccessful candidates: up to 24 months unless renewed consent or legitimate interest applies
- Placed candidates: retained for legal, contractual and compliance purposes
- Client records: retained for ongoing business relationship management

Full retention details are set out in the Company's Data Retention Policy.

13. Secure processing

The Company implements appropriate security measures including:

- Controlled access to systems
- Password protection and authentication controls
- Encryption where appropriate
- Restricted access on a need-to-know basis
- Secure storage of digital and physical records

Security measures are regularly reviewed and updated.

14. Accountability and record keeping

The Company maintains records of processing activities including:

- Purposes of processing
- Categories of data subjects and data
- Lawful bases for processing
- Data sharing arrangements
- Retention schedules
- Security measures

Staff receive appropriate data protection training, which is completed annually or earlier if upon review required.

15. Data protection impact assessments and privacy by design

Data Protection Impact Assessments are carried out where processing is likely to result in high risk to individuals.

The Company adopts privacy by design principles when introducing new systems or processing activities.

Factors considered include:

- Nature and scope of processing
- Sensitivity of data
- Risks to individuals
- Security controls and safeguards

16. Keeping data subjects informed

Data subjects are provided with privacy information including:

- Identity and contact details of the Company
- Purpose and lawful basis of processing
- Retention periods
- Data sharing arrangements
- International transfers
- Individual rights
- Right to complain to the ICO

17. Subject access requests

Data subjects may request access to their personal data at any time.

Requests must be submitted to the Data Protection Officer.

The Company will respond within one month, extendable where necessary.

Excessive or unfounded requests may be refused or charged in accordance with UK GDPR.

18. Rectification of personal data

Data subjects may request correction of inaccurate or incomplete personal data.

The Company will respond within one month.

19. Erasure of personal data

Data subjects may request erasure of their personal data where:

- It is no longer necessary
- Consent is withdrawn
- Processing is unlawful
- There is a legal obligation to erase

20. Restriction of personal data processing

Data subjects may request restriction of processing in certain circumstances.

Where applied, data will be stored but not further processed.

21. Data portability

Where applicable, data subjects may request their personal data in a structured, commonly used electronic format.

This will usually be provided in electronic format such as PDF or CSV.

Where technically feasible, data may be transferred directly to another controller.

22. Objections to personal data processing

Data subjects may object to processing based on legitimate interests or direct marketing.

The Company will cease processing unless compelling legitimate grounds override the objection.

23. Automated decision making and profiling

The Company uses limited automated assessment within its CRM system to assist candidate suitability matching.

All decisions are subject to human review and do not produce solely automated legal or significant effects.

Data subjects may request human intervention and object to profiling.

24. Direct marketing

The Company may conduct direct marketing in compliance with UK GDPR and PECR.

Individuals are provided with clear opt-out options and can withdraw consent at any time.

25. Personal data collected, held and processed systems

The Company processes personal data using:

- Applicant tracking systems (ATS)
- Customer relationship management (CRM) systems
- Email and communication platforms
- Cloud storage systems
- Payroll and finance systems (where applicable)

All systems are subject to access controls and security measures.

26. Transfers of personal data outside the UK

Personal data may be transferred outside the UK only where appropriate safeguards are in place, including:

- UK adequacy regulations
- Standard contractual clauses
- Explicit consent where required
- Other lawful transfer mechanisms under UK GDPR

27. Data breach notification

All personal data breaches must be reported immediately to the Data Protection Officer, Abbie Cavanagh (abbie@standbyhealthcare.com, 0191 646 0100).

Where a breach is likely to risk individuals' rights and freedoms, it will be reported to the ICO within 72 hours.

Where there is a high risk, affected individuals will be notified without undue delay.

28. Information commissioner's office (ICO)

Data subjects have the right to lodge a complaint with the UK supervisory authority if they believe their personal data has been misused or their data protection rights have not been upheld.

The supervisory authority in the United Kingdom is:

Information Commissioner's Office (ICO)

Website: <https://ico.org.uk>

Data subjects may contact the ICO directly for advice or to raise a concern regarding the processing of their personal data by the Company.

The Company encourages individuals to contact the Data Protection Officer in the first instance so that concerns can be addressed internally.