Policy

Information Governance and Data Protection Policy

This policy applies to all data sharing activities within the Voyage Care group

Document information			
Classification	Policy	Version	4.0
Owner	Legal Director and Company Secretary	Release date	January 2025
Author	Legal team	Review date	January 2027
If printed this document is uncontrolled. Always check the intranet for the latest version.			

Contents

1 Introduction

Information Governance gives assurance to all Voyage Care stakeholders including the people we support, their families and our colleagues that personal information is dealt with legally, securely and efficiently in order to deliver the best possible care.

Voyage Care recognises that it is important to ensure that personal information and confidential company data is effectively managed and that appropriate policies, procedures, management accountability and structure provide a robust governance framework for data protection and comply with all data protection regulations.

This document is applicable to all company confidential data and data we hold on behalf of the people we support and Voyage Care colleagues.

2 Aim of the Policy

The aim of this policy and the procedures connected to this policy is to provide Voyage Care colleagues with the guidelines necessary to comply with the UK General Data Protection Regulations (also referred to in this policy as "GDPR") requirements.

3 Responsibilities and governance

The Voyage Care Holdco Limited Board of Directors and the Chief Executive Officer (CEO) have ultimate accountability and responsibility for the safety of all colleagues and the people that we support, which includes compliance with GDPR. This responsibility is delegated through organisational structures and accountability frameworks in order to ensure colleagues providing direct or delegated care and support are provided with the appropriate tools and training to undertake their duties.

Legal Director, Company Secretary and Data Protection Officer is accountable for this policy and when requested, for providing assurance reports, identifying its effectiveness to the quality, safety and risk committee. The company board may request assurance from the Legal Director that appropriate structures are in place and that colleagues are provided with appropriate training and resources to undertake their duties.

The Executive Committee of Directors of the Company and the Managing Directors are accountable for promoting awareness of the policy and ensuring when required, suitable colleagues training and review of competence in relation to all matters associated with this policy.

The Quality, Safety and Risk Committee are a sub group to the Board of Directors and are responsible for requesting and receiving assurance reports relating to GDPR, when required, regarding the application and effectiveness of this policy and related procedures and procedural documents.

Registered/Service Managers/Branch/Clinical Managers/Operations Managers and Operations Directors are responsible for ensuring this policy is implemented and complied with across their services. This includes:

- Compliance with training and record keeping;
- Ensuring all colleagues practice within their sphere of responsibility and attend training on this policy where appropriate;
- Ensuring that this policy is fully implemented, and all required documentation is completed;
- Ensuring all requirements of this policy are monitored through audit, where appropriate;
- Taking action with individual Colleagues where necessary when the policy is not adhered to.

Colleagues (includes bank and agency), all colleagues including colleagues who work at Group Support offices and volunteers have an on-going responsibility to identify their own training needs in conjunction with their co-ordinator / line manager / supervisor, job description and service. This must be acknowledged within the appraisal system.

4 Scope

This policy (and the policies and procedures connected to this policy) apply to Voyage Care's compliance with the UK General Data Protection Regulations other data protection legislation (see section 5), and other matters relating to data protection and privacy. This policy covers all areas of Information Governance within Voyage Care including (but not limited to):

- Clinical information assurance;
- Confidentiality and data protection;
- Governance of the flow of personal data and confidential information across Voyage Care;
- Information security;
- Data Protection training;
- Records and storage management;

- Structured record systems – paper and electronic;
- Processing and manipulation of data – manual and automated;
- Transmission of information – fax, e-mail, post and telephone;
- Privacy and Consent;
- How paper records are managed; and
- Physical controls in buildings to secure documents

This policy covers all information systems purchased, developed and managed by or on behalf of Voyage Care.

All aspects of this policy apply to all sites operated by Voyage Care and to the extent that is possible, all supported living premises wherein we provide support, as well as all those having access to information, such as Colleagues and any third parties such as contractors, students, locums, and visitors.

This policy also refers to more specific policies on certain topics.

5 Data Protection aims and principles

Voyage Care adheres to the following principles in line with the UK GDPR:

- **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date.
- **Storage Limitation:** Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary.
- **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- **Accountability**: Voyage Care is responsible for, and must be able to demonstrate, compliance with all these principles.

6 Security Controls

A comprehensive set of controls, monitoring, processes, and policies are in place providing a multi-layered cyber security defence strategy to keep personal and sensitive data safe, prevent security incidents and to monitor and respond to security incidents in the event they occur. These include Firewalls, VPN, anti-virus, email scanning, web filtering and end-point protection.

External standards and benchmarks are increasingly being proactively employed to further improve our security posture against industry best practice, and to meet the increasing requirements of cyber security insurance, commissioners, and the NHS.

Additional defences are being continually identified and, subject to appropriate business cases, being introduced to harden defences and further improve our ability to protect data and systems.

7 Lawful, Fair and Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;
d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
e) the 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 data controller; or
f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
c) the 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) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
e) the processing relates to personal data which is manifestly made public by the data subject;
f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
i) the processing is necessary for public interest reasons in the area of public health, for example, 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 law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as

supplemented by section 19 of the Data Protection Act 2018) based on 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 Data Subject Rights

Voyage Care recognises and upholds the rights of data subjects under the UK GDPR, including:

- **Right to be Informed**: Individuals have the right to be informed about the collection and use of their personal data.
- **Right of Access**: Individuals have the right to access their personal data and obtain a copy of it. (For further information see the Data Subject Request Policy and Procedure)
- **Right to Rectification**: Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.
- **Right to Erasure (Right to be Forgotten)**: Individuals have the right to have their personal data erased in certain circumstances.
- **Right to Restrict Processing**: Individuals have the right to request the restriction or suppression of their personal data.
- **Right to Data Portability**: Individuals have the right to obtain and reuse their personal data across different services.
- **Right to Object**: Individuals have the right to object to the processing of their personal data in certain circumstances.
- **Rights Related to Automated Decision-Making and Profiling**: Individuals have the right not to be subject to a decision based solely on automated processing, including profiling.

Voyage Care's relevant Privacy Notices provide further details on how individuals can exercise their rights in relation to the way that the company processes their data.

9 Accuracy of Data

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

10 Data Retention

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to destroy or pseudonymise without delay.

For full details of the Company's approach to data retention, including retention periods for specific personal data, please refer to our Record and Retention Procedure.

11 Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

Please refer to the Data Protection Impact Assessment policy & procedure for further details.

12 Subject Access Requests

Individuals may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

Individuals wishing to make a SAR should do so by emailing SAR@voyagecare.com.

All SARs received shall be handled by the Company's Data Protection Officer and Legal Team in accordance with the Subject Access Request Policy & Procedure**.**

13 Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

14 Erasure of Personal Data

Data subjects have the right to request that Voyage Care erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;
c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);
d) the personal data has been processed unlawfully;
e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation
f) the personal data is being held and processed for the purpose of providing information society services to a child.

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

15 Restriction of Personal Data Processing

Data subjects may request that Voyage Care ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

16 Data Breach Management

A data breach occurs when there is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This can happen as a result of various factors, including:

- **Cyberattacks**: Such as hacking, ransomware, or phishing.
- **Human Error**: For example, sending personal data to the wrong recipient, losing a device containing personal data, or inadvertently making data publicly accessible.
- **Physical Breach**: Loss or theft of devices or documents containing personal data.
- **System Malfunction**: Failures or vulnerabilities in IT systems that expose personal data to unauthorised access.

Data breaches can compromise the confidentiality, integrity, or availability of personal data and may result in significant harm to individuals, including identity theft, financial loss, or reputational damage.

By following the Data Breach Management Policy & Procedure, Voyage Care ensures a prompt and effective response to data breaches, minimising harm and fulfilling its legal obligations under the UK GDPR.

17 Data Quality

Voyage Care recognises that the quality, accuracy and completeness of data is important so that there is confidence in decision-making processes and strength in the relationship with the People we Support, Colleagues, customers, suppliers, processors and other stakeholders.

Voyage Care uses reasonable endeavours to maintain accurate and up-to-date information and particular care is taken to ensure that sensitive information that may have a negative impact on the People we Support or Colleagues is accurate.

Voyage Care ensures that personal data that cannot reasonably be assumed to be accurate and up-to-date is treated appropriately through erasure or anonymisation. Anonymisation is the process of either encrypting or removing personally identifiable information from data groups, so that the people whom the data describes remains anonymous.

18 Legislation

Voyage Care will comply with the following and other legislation as appropriate:

- The Data Protection Act 2018 and the General Data Protection Regulations (2018);
- The Copyright, Designs and Patents Act (1988);
- The Computer Misuse Act (1990);
- The Health and Safety at Work Act (1974);
- Human Rights Act (1998);
- Regulation of Investigatory Powers Act (2000);
- Health and Social Care Act (2012);
- The Care Act (2014)
- Social Work Scotland Act 1968 (which was reinforced by the Social Care (self-directed support) (Scotland) Act 2013); and
- The Social Services and Well-being (Wales) Act 2014

And all subsequent amendments.

19 Training

Voyage Care offer a mandatory Handling Information e-learning course course which covers: GDPR, The Data Protection Act, Caldicott Guardian and the Accessible Information Standard. This course is required to be completed every 3 years.

A Data Protection Training Needs Analysis will be completed annually. A Data Protection Training Needs Analysis helps us identify the training needs of all Colleagues in relation to data protection and cyber security.

20 Document review and revision

The Company undertakes to review all documented policies and procedures every two years.

The Company will additionally review all documentation:

- Where investigations into complaints and incidents indicate a change is required;
- Where customer feedback informs of change;
- For improvements to the service as a result of employee suggestions;
- Changes arising from safeguarding or equality and diversity issues;

- As a result of changes in legislation or recommendations from the NHS or recognised clinical bodies.

All policy and procedure documents will display both release and review dates.

Responsibility for ensuring review rests with the Legal Director (Company Secretary and Data Protection Officer).

21 Document Control

Only the last 12 months of document control is detailed within our Policies and Procedures. Older versions are archived and available to view on request.

Date	Version	Section	Revision details	Revised by
January 2025	4.0	All	Whole document review. Revise formatting and remove typos Added link to the reinstated Data Protection Impact Assessment Policy and Procedure. This is due to be reviewed by the Legal team in January 2025.	Legal Team