STELLAR
HEALTHCARE

Information Governance Policy

1. Introduction

Information is a critical asset for delivering high-quality care to service users, ensuring quality assurance, and managing services and resources efficiently. Stort Valley Healthcare Ltd is committed to maintaining a robust information governance (IG) framework to protect and manage information in compliance with NHS standards, the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), and other relevant legislation.

2. Purpose of the policy

This Information Governance Policy outlines Stort Valley Healthcare Ltd's approach to information governance, provides guidance on procedures, and details the management structures overseeing these arrangements. It ensures compliance with the NHS Data Security and Protection Toolkit (DSPT), Caldicott Principles, and statutory obligations, fostering trust in how we handle personal and sensitive information.

3. Our approach to Information Governance

Stort Valley Healthcare Ltd undertakes to implement information governance effectively and will ensure the following:

- **Information Sharing:** Information will be shared lawfully and securely with partner organisations to facilitate high-quality care, supported by formal data sharing agreements compliant with GDPR and NHS guidelines
- **Security:** Information will be held securely in line with the NHS Data Security Standards and protected against unauthorised access, loss, or damage.
- **Confidentiality:** Confidentiality of personal and sensitive data will be assured, adhering to Caldicott principles and GDPR
- **Data Quality:** Information will be accurate, complete and up to date to support effective care and decision-making.
- **Compliance:** All regulatory and legislative requirements, including GDPR, DPA 2018 and the Freedom of Information Act 2000, will be met.
- **Business continuity:** Robust business continuity plans will be developed, maintained, and tested to ensure service delivery during system failures or other disruptions.
- **Training:** All staff will receive mandatory annual Data Security Awareness Training and role-specific guidance to ensure compliance with IG policies.
- **Incident Management:** All actual or suspected breaches of confidentiality or information security will be reported, investigated and where required, notified to the Information Commissioner's Office (ICO) within 72 hours, as per GDPR requirements.
- **Cybersecurity:** Robust cybersecurity measures, including encryption, access controls and regular security assessments will be implemented to protect data.

4. Procedures in use in the organisation

This policy is underpinned by the following procedures, aligned with NHS DSPT requirements:

- **Records management procedures**: Define how records are created, used, stored and disposed of in compliance with the Records Management Code of Practice for Health and Social Care 2021
- **Access control procedures:** Ensure secure access to computer-based information systems, including role-based access controls and multi-factor authentication where appropriate.
- **Information handling procedures:** Outline secure methods for transferring information, including encrypted email and secure file transfer protocols.
- **Incident management procedures:** Detail processes for identifying, reporting and managing information incidents, including mandatory reporting to the ICO and NHS Digital via the DSPT Incident Reporting Tool**.**

- **Business continuity procedures:** Support service delivery in the event of system failures, cyber incidents or other disruptions.
- **Data Sharing Procedures:** Ensure lawful and secure sharing of data with partner organisations through formal agreements compliant with GDPR and NHS standards.

5. Staff training and guidance

All staff will complete mandatory NHS Data Security Awareness Training annually, with additional role-specific training provided as needed. Compliance with IG procedures will be monitored through regular audits, and additional support or training will be provided where gaps are identified. Staff will have access to up-to-date guidance on data protection, confidentiality, and secure information handling.

6. Responsibilities and accountabilities

The designated **Information Governance Lead** for Stellar Healthcare is Chris Mitchell. Their key responsibilities include:

- Completing and submitting the annual Data Security and Protection Toolkit (DSPT) assessment, ensuring honest and comprehensive evaluation of IG performance
- Maintaining and updating the IG Policy and associated procedures to reflect NHS and legislative requirements.
- Raising awareness and providing advice and guidance on IG to all staff.
- Ensuring all staff complete mandatory training and that additional training is provided where necessary.
- Coordinating the activities of staff with responsibilities for data protection, confidentiality, information quality, records management and Freedom of Information.
- Monitoring adherence to IG procedures and conducting regular audits.
- Reporting data breaches to the ICO within 72 hours and to NHS digital via the DSPT incident reporting tool, as required.
- Liaising with the Caldicott Guardian to ensure compliance with Caldicott Principles.

The organisation, through its directors, is responsible for:

- Providing sufficient resources to support effective IG implementation.
- Ensuring compliance with the NHS Information Governance Assurance Framework, DSPT, GDPR and DPA 2018
- Appointing a Senior Information Risk Owner (SIRO) to oversee information risk management.

All **staff**, whether permanent, temporary or contracted, and contractors are responsible for:

- Familiarising themselves with and adhering to this policy and supporting procedures
- Completing mandatory training and applying guidance in their roles
- Reporting any actual or suspected information incidents promptly. Failure to comply with IG policies and procedures may result in disciplinary action.

7. Approval

This policy has been approved by the Board of Directors and will be reviewed biennially or as required to ensure continued compliance with NHS and legislative standards.