DATA PROTECTION POLICY

Created	**July 2019**
Review Date	**July 2023**
Next Review Date	**July 2024**
Author	**Director of Quality and Governance**
Authorised By	**Chief Executive Officer**
Distribution	**All Staff**
Available to	**All Staff**

Signed ……

July 2023

Signature Dated ……

Change Control

Document Number	GOV – SVL0030 – Policy
Document	Data Protection Policy
Version	5
Owner	Director of Quality and Governance
Distribution List	All Staff
Issue Date	July 2019
Next Review Date	July 2024
File Reference	GOV – SVL0030 – Policy
Impact Assessment	Positive Impact
Author	Director of Quality and Governance

Document History

Date	**Change**	**Authorised by**
July 2019	Review and Amended	LB
15/07/2019	Approved and Implemented	SMT
July 2020	Review and Amended	LB
July 2021	Review and Amended	LB
July 2022	Reviewed and amended	LB
July 2023	Reviewed and amended	LB

Contents **Page**

1 Policy Statement

SVL Healthcare Services Limited (SVL) has made every effort to ensure this Policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of age, disability, gender reassignment, race, religion/belief, gender sexual orientation, marriage/civil partnership, pregnancy/maternity. The Company will not tolerate unfair discrimination based on spent criminal convictions, Trade Union membership or non-membership. In addition, the Company will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to individuals working at all levels for the Company, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed term or temporary) consultants, contractors, trainees, casual workers and agency staff, volunteers, interns or any other person associated with the Company.

The Company is fully committed to compliance with the requirements of the Data Protection Act 2018, The General Data Protection Regulation (GDPR) and is registered with the Information Commissioner's Office (ICO – Z1172873).

SVL is compliant with the NHS Data Security Protection Toolkit (Registration number: 8HY24) Our 2022 assessment is published via NHS Digital.

The Company will therefore follow procedures which aim to ensure that all employees, contractors, instructors, agents, consultants, partners, or other servants who have access to any personal data held by or on behalf of the service, are fully aware of and abide by their duties under the Data Protection Act 2018 and GDPR.

It also complies with the Caldicott Principles2 concerning Patient Identifiable Information (PII) and the requirements of the NHS Data Security and Protection Governance Toolkit. This includes the specific requirements and challenges surrounding Safeguarding of Children and Vulnerable Adults and data transfer and sharing requirements of NHS and Social Care provision by the Company.

This Policy should be read in conjunction with the Company Information Governance & Security Policy, Information Sharing Policy, and associated documents.

2 Background

To operate efficiently, The Company has to collect and use information about people with whom it works. This may include members of the public, current, past, and prospective employees, patients, clients, customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central government.

This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to assure such.

The Company regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between itself and

those with whom it carries out business. The Company will ensure that it treats personal information lawfully and correctly.

To this end the Company fully endorses and adheres to the 8 principles of Data Protection as set out in the Data Protection Act 2018.

3 Purpose

The Company is committed to adhering to best practice regarding Information Governance and the protection of data. The purpose of the Data Protection Act and the GDPR is to protect the rights of individuals about whom data (information) is obtained, stored, processed, and disclosed.

4 Legislation

The Data Protection Act 2018 GDPR came into force in May 2018 and is linked with other legislation and guidance to include:

- The Freedom of Information Act 2000 (with regards to public funded services only)
- Health and Social Care Information Centre Code of Practice on confidential Information
- Records Management code of Practice for Health and Social Care 2016; including appendix 3 retention schedule.
- NHS and Social Care Information Governance Toolkit
- Caldicott2 Principles
- Confidentiality: NHS Code of Practice
- Information Security Management: NHS Code of Practice.

There are legislative requirements to data protection and data sharing within the Children's Act 1989/2004 Health & Social Care Act 2008 / (Regulations 2014) and various crime and disorder legislation and guidance.

All the above need to be managed within the law.

The Company has procedures in place for the storage and destruction of data and data sharing agreements.

The Principles of Data Protection

The Data Protection Act 2018 stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The principles require that personal information:

1. Personal data shall be processed fairly and lawfully and, shall not be processed unless:
    - At least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met, and
    - In the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act 2018 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.
4. Personal data shall be accurate and where necessary and kept up to date.
5. Personal data shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal date shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidents loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

The Caldicott2 Principles

The Caldicott2 Principles set out the following conditions in the collection; use; processing; retention of all data:

1. Justify the purpose of using or transferring personal confidential data.
2. Do not use personal confidential data unless it is necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Understand and Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data and other information which is in the possession of or is likely to come into the possession of the Data Controller and includes an expression of opinion about the individual and any indication of the intentions of the Data Controller, or any other person in respect of the individual.

"Sensitive" personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal or alleged offences
- Criminal proceedings, convictions or disposal of proceedings

5 Scope

This policy relates to all information held within the organisation in any format.

6 Handling of Personal/Sensitive Information

The Company will, through robust procedures, education, management, and appropriate structure.

- Observe fully conditions regarding the fair collection and use of personal information meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Assure the quality of information.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred without suitable safeguards.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
- At the end of any contract SVL will complete necessary authorised destruction of data that does not require legal retention. This will be completed by accredited security shredding.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.

- The right to correct, rectify, block or erase information regarded as wrong information.

7 Structure and Accountabilities

The Company, via the Executive Board (EB), is required to discharge its responsibilities under the Data Protection Act 2018 and GDPR in relation to the collection, protection, safe use, and disposal of information ensuring the safety of its staff, the general public and the environment.

Director of Quality and Governance

The post holder has the overall responsibility, on behalf of the Executive Board, to ensure that this Policy is implemented throughout the Company, and:

- Will maintain registration with the Information Commissioner's Office.
- Will be directly responsible for the establishment and continued development of the Company data protection processes to ensure IG Toolkit requirements.
- Will be responsible for monitoring the effectiveness of the arrangements made to implement this policy.
- Will report any data breaches to the Information Commissioner's Office, other organisations and the individuals concerned, as appropriate.

Data Controller

The post holder is responsible for ensuring that all information and technical systems:

- Are safe and secure regarding electronic storage of data.
- There is a clear and robust encrypted password protected system in place regarding the main server, through individual user file security and individual documents and access.
- There are clear technical processes in place for secure telecommunication systems.
- There are robust and secure backup and contingency processes in place for secure data safety.
- The review and updating of SVL policies is completed including the processing of data and the data controller is advised and updated accordingly.
- The necessary policies are implemented operationally with effective communication pathways and accessibility to information relating to this Policy is made available to all staff within the Company.
- Suitable and effective risk assessments are undertaken for the use, storage and disposal of operational data and that they form the basis for establishing safe systems of work in accordance with regulatory requirements.
- Access is made available to operational staff for suitable and sufficient training required under Data Protection Act 2018.

All Directors

All Directors are responsible for ensuring the implementation and application of this Policy within their own Directorate and will ensure that:

- The Executive Board (EB) is advised on an on-going basis, of any risks associated with their respective areas of responsibility and that all associated managers and staff receive any necessary training and information to ensure safe practice throughout their Directorate.

Operational Managers

All Operational Managers are responsible for the continued application of data protection throughout their area of responsibility. These duties include:

- Ensuring all staff are supported in the use of data and all relevant information is made available to ensure their awareness in the use of data and their responsibilities under the Data Protection Act 2018.
- Ensuring all incidents and near misses relating to data and information are reported and accurately recorded and processed in accordance with statutory requirements and Company procedures.
- Undertaking investigations when required regarding incidents involving possible data breaches and ensure all details are accurately documented and appropriate action is taken to prevent any recurrence.
- Ensuring, where necessary, risk assessments regarding data and information are carried out.
- Ensuring that controls are in place to prevent the access to and the use of unauthorised data within their area of responsibility.

Employees

All employees will:

- Make themselves familiar with this Policy and associated safe working processes.
- Assist management to ensure compliance with the Data Protection Act 2018.
- Take care of their own information governance processes (including the safe handling of passwords etc., and of those who may be affected by their acts or omissions).
- Report all accidents, dangerous occurrences and near misses directly to their Line Manager (see Incident Reporting and Investigation Policy).

- Keep all paper files and other records or documents containing personal/sensitive data in a secure environment.
- Ensure that all personal data held on computers and computer systems is protected using secure passwords which, where possible and practicable, have mandatory periodic changes.
- Ensure that individual passwords are such that they are not easily compromised.

Contractors and Others

All contractors, consultants, partners or other servants or agents of the Company must:

- Ensure that they and all their staff who have access to personal data held or processed for or on behalf of SVL are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm.
- Allow data protection audits by the Company of any data held on its behalf (if requested).
- Indemnify the Company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the Company will be required to confirm that they will abide by the requirements of the Act regarding information so supplied.

8 Data/Information Breaches or Near Misses

All staff will be aware of the definition of a data breach or near miss and their requirement to report this as part of the Data/Information Breach procedure using the SVL Incident Reporting process. The Director of Quality and Governance will initiate and appoint an investigating officer and report the incident as appropriate according to the procedure. Any incident deemed as a Serious Incident will be managed by the Director of Quality and Governance and reported to the Information Commissioner's Office, the appropriate Commissioner, the Care Quality Commission, and the Company's Insurers, as appropriate**.**

9 Notification to the Information Commissioner

The Data Protection Act 2018 requires every organisation that is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end, the designated officers will be responsible for notifying and updating the Data Protection Officer of the processing of personal data within their directorate.

The Data Protection Officer will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner's Office.

Any changes to the register must be notified to the Information Commissioner's Office, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Data Protection Officer immediately.

10 Information Sharing

10.1 Request of Information – Personal

The Data Protection Act 2018 and the GDPR gives individuals the right to apply for a copy of their personal information. The subject access request must be in writing, by letter or email, and on receipt will be considered by the Chief Executive and/or the Director of Quality and Governance.

Applicants will be informed accordingly and that the Company may not charge an administration fee under GDPR requirements unless the requests are in excess from any individual. A response will be provided within one month.

10.2 Information Sharing with Other Organisations

The Company recognises its requirement to share information with other organisations. This may result from legislative or contractual requirements.

The Company will share and transfer information according to its Information Sharing Policy.

10.3 Freedom of Information Requests

These will be considered by the Chief Executive or designate following the Freedom of Information Act Policy.

11 Policy Review

This Policy will be reviewed every year or amended in the light of new legislation and/or relevant case law, or changes to associated SVL policies.

12 Source

In compiling this Policy, reference has been made to the following sources: -

11.1 Data Protection Act 2018 & the General Data Protection Regulation 2018 (GDPR)
11.2 Caldicott2 Principles
11.3 Freedom of Information Act 2000
11.4 Health and Social Care Information Centre Code of Practice on confidential information.
11.5 Records Management Code of Practice for Health and Social Care 2020,
11.6 NHS and Social Care Information Governance Toolkit
11.7 Confidentiality: NHS Code of Practice
11.8 Children's Act 2004 (1989 development)
11.9 Heath and Social Care Act 2012

Appendix A

Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	

		Yes/No	Comments
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to Director of Quality and Governance, together with any suggestions as to the action required to avoid/reduce this impact.

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?		
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	

	Title of document being reviewed:	Yes/No/ Unsure	Comments
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	Email staff
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	Archived in folder store on server
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	Internal auditor
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	

	Title of document being reviewed:	Yes/No/ Unsure	Comments
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation, and review of the document?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the Chief Executive Officer where it will receive final approval.			
Name	Brian Wren	Date	July 2023
Signature			
SMT Approval			
If the SMT is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Lee Barham	Date	July 2023
Signature