Third-party Suppliers Data Protection & Security Assurance Policy

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	The purpose of this policy is to ensure that the Trust and its contractors meet their legal requirements, as outlined by the Data Protection Legislation, with regards to the procurement and contracting of services, involving the processing of Personally Identifiable Data
Document Type	Policy
Linked to O-SOP	N/A
Reference Number	Solent NHST / Policy / IG24
Version	V1
Name of Approving Committees / Groups	Policy Steering Group, Clinical Executive Group
Operational Date	May 2022
Document Review Date	May 2025
Document Sponsor (Job Title)	Senior Information Risk Owner
Document Manager (Job Title)	Data Protection Officer and Head of Information Governance & Security
Document developed in consultation with	Commercial and Procurement Teams
Intranet Location	Business Zone > Policies, SOPS and Clinical Guidelines
Website Location	Policies and Procedures – Publication Scheme
Keywords (for website/intranet uploading)	Data Protection, Commercial, Contract, Procurement, Third-party Supplier, Policy, IG24

Review and amendment log

Version Number	Review date	Amendment section no.	Page	Amendment made / summary	Changes approved by
1	New Policy				Policy Steering Group, Clinical Executive Group

SUMMARY OF POLICY

The purpose of this policy is to ensure that all contracts and agreements between the Trust and third-party suppliers have acceptable levels of information security and information governance processes to ensure that personal and sensitive data is protected and managed in line with statutory and good practice requirements.

The policy aims to ensure that both the Trust and its Third-Party Suppliers met their legal obligations, under Data Protection Legislation.

The policy outlines the responsibilities and actions required of the:

- Executive Leadership Team
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owners
- Information Governance Team
- Procurement / Commercial Team

Table of Contents

THIRD-PARTY SUPPLIERS DATA PROTECTION & SECUIRTY ASSURANCE POLICY

1. INTRODUCTION & PURPOSE

1.1 Solent NHS Trust (hereafter referred to as "the Trust") relies on the integrity and accuracy of its information to deliver its services. It is therefore paramount that the integrity, confidentiality, and availability of its information are ensured, throughout the lifecycle of that information.

1.2 In order to provide effective health services, the Trust will need to enter into contracts and agreements with outside organisations. For the purposes of this policy, these organisations will be referred to as 'third-party suppliers'. These third-party suppliers may be primary or sub-contractors or relate to any other party (including individuals or sole traders) that the Trust enters into an agreement with to provide services to our patients.

1.3 Information and information systems are vital assets of the Trust's. It is essential that the organisation has the appropriate technical and security measures in place to protect this information. This requirement becomes increasingly important in the case of patient, staff and other sensitive information and where there is a requirement to share this information with third parties who are delivering services on behalf of the Trust.

1.4 The purpose of this Policy is to ensure that:

- Third-party suppliers have acceptable levels of information security and information governance processes to ensure that personal and sensitive data is protected and managed in line with statutory and good practice requirements.
- All Trust information is appropriately managed and processed by those Third Parties with which that information is shared, or by which that information is handled.
- Third-party suppliers understand, and adhere to, all relevant Policies regarding information security and associated security constraints established by the Trust.
- The Trust maintains the confidence of all relevant stakeholders and remains in compliance with legal and regulatory requirements.

1.5 The aim of this policy is to ensure that the Trust complies with its statutory duties laid out in the Data Protection Act 2018 / General Data Protection Regulations 2016 or any subsequent legislation to the same effect, the Human Rights Act 1998 and with the common law duty of confidentiality. It will ensure that all third-party organisations who enter into an agreement or contract with the Trust are clear about the Trust's expectations in terms of information security and confidentiality. It will ensure that both the Trust and any organisation acting as a data processor for the Trust, will have the relevant technical and security measures in place to meet data protection legislation and privacy requirements. The correct application of this policy will ensure that the Trust is compliant with its legislative responsibilities, reduce the risk of an information security breach taking place, and provide assurance to our staff and patients that information assets are being properly managed.

1.6 All third-party suppliers shall comply with the Trust's Data Protection Compliance Policy, legal obligations, and associated documentation. Any exemptions shall be specifically written and agreed within the third-party supplier's contract. All contractors will be required to provide annual assurance of compliance with Data Security Protection Toolkit, Data Protection Training and are subject to random spot-check audits by the Trust.

2. SCOPE & DEFINITIONS

2.1 This policy applies to:

- The Executive Leadership Team
- Senior Information Risk Owners
- The Caldicott Guardian
- Information Asset Owners
- Information Governance Team
- Procurement / Commercial Team
- Third Party Suppliers in so far as being compliant within the terms of their contract with the Trust and for ensuring their compliance with UK laws and regulation

2.2 Solent NHS Trust is committed to the principles of Equality and Diversity and will strive to eliminate unlawful discrimination in all its forms. We will strive towards demonstrating fairness and Equal Opportunities for users of services, carers, the wider community, and our staff.

2.3 This policy covers all aspects of personal information within the Trust, including but not limited to:

- Patient / client / service user information
- Personnel and staff information
- Sensitive corporate information

3. ROLES & RESPONSIBILITIES

3.1 **Executive Directors**: Executive Directors are responsible for the overall management of information risk within their service areas and are responsible for ensuring their staff and managers are aware of this policy.

3.2 **The Senior Information Risk Owner and Caldicott Guardian**: The Senior Information Risk Owner and Caldicott Guardian are responsible for managing information risk and the safe and ethical use of information across the Trust and are responsible for ensuring their staff and managers are aware of this policy.

3.3 **Information Asset Owners:** Information Asset Owners are responsible for understanding what information is held within their service areas and where contracts and agreements are being entered into with third-party suppliers involving the sharing of, or access to Trust information. These arrangements with third-party suppliers are to be listed on the Trust's information asset registers.

Information Asset Owners are able to delegate this responsibility to another named individual within their service area, but they must retain overall responsibility for ensuring that this policy is followed when any of their services (via the Trust's Commercial Team) enter into a third-party contract or agreement.

3.4 **Information Governance Team**: The Information Governance Team are responsible for disseminating this policy across the Trust and ensuring it is readily available to all staff. The team are responsible for providing appropriate support and advice to Directors, Information

Asset Owners, Service Leads, Procurement & Commercial Team, staff, and managers to ensure the policy is understood and adhered to.

The Information Governance Team are also responsible for ensuring the following is undertaken, with regards to due diligence of all third-party suppliers, who process personal data:

- Data Protection Impact Assessment is undertaken.
- Third Parties Information Security and Data Protection Compliance is assessed.
- Assessment is undertaken to ensure that any supplier of ICT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.
- Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.
- All third-party suppliers that process or have access to personal confidential health or care information, have completed a Data Security and Protection Toolkit, or equivalent.
- All contracts with third-party suppliers include the necessary data security clauses.

3.5 **Procurement & Commercial Team**: The Procurement & Commercial Team are responsible for ensuring that the appropriate Third-party Supplier Security Questionnaire is sent to potential suppliers as part of the procurement process and that any contracts sent via their team, meet the minimum requirements as laid out in this document. Where any officer of the Trust has not sought a third party supplier via usual procurement routes, the relevant Director will be responsible for alerting the Procurement and Commercial Team to its existence in order that the relevant checks and documentation can be established as soon as possible.

The Procurement Team will also be responsible for ensuring the following is undertaken, with regards to all contractual relationships between the Trust and the Third-party Supplier;

Prior to engagement:

- Third-party Suppliers whose engagement with the Trust will entail use of the Trust's ICT and / or handling or processing of its information, shall have established a management framework for information security and risk which is signed off at the appropriate level, and which ensures the necessary resources to provide required controls.
- Documented procedures shall be in place to authorise significant changes to agreed information processing procedures for the Trust, and to ensure relevant information, security contracts and controls are maintained.
- Third-party Suppliers personnel shall be subject to appropriate background and vetting checks, depending upon their roles and access levels.

Contractual Arrangements:

The Commercial Team are responsible for issuing contracts to third parties, that outline the following:

- The third-party supplier's legal obligations and accountabilities under Data Protection Legislation
- The third-party supplier's legal obligation to report all Data Protection Breaches within 72 hours
- The Trust's rights and obligations to undertake Security Audits against the third-party suppliers processing activities
- The third-party supplier's obligation to maintain security accreditation

- The third-party supplier's obligation to notify the Trust of any changes to processing activities

During engagement:

- Trust information processed and handled by Third Parties shall, as a minimum, be classified and handled in accordance with the Trust's Data Protection Compliance Policy; this activity is supported and reviewed by the Trust's Data Protection Officer and then defined within the Third Parties Contract.
- Third-party Supplier Facilities and Equipment shall be secured to prevent loss, damage, theft, or compromise of Trust information assets.
- Access control shall be implemented.
- Third-party Suppliers shall ensure that appropriate information security awareness, training and education is in place for their personnel to meet contractual requirements.
- Where individual personnel of the Third party, who has been given access to Trust systems or data, has changed role, or is terminated from employment in the course of the contract, the Third-party shall:
  - inform the Trust of that change in personnel
  - ensure that any passes are returned
  - ensure that any ICT equipment issued by the Trust is logged and returned to the Trust
  - provide details of personnel replacement for vetting as appropriate
- Third-party Suppliers shall comply with contractual obligations to assist any information security audits undertaken by the Trust or nominated parties.
- In the event of breach or data loss regarding the Trust's information, Third Parties shall observe the Trust's Data Protection Compliance Policy and bring matters directly to the attention of the Trust's DPO. This is to be reported to the Trust within 72hrs.

Termination or change of engagement

- Third-party Suppliers shall ensure that the integrity, availability, and security of information belonging to, or processed, or held on behalf of the Trust, is maintained throughout any change of roles or ongoing contractual management.
- Third-party Suppliers shall ensure that details are provided to the Trust such that:
  - any access or permissions to access the Trust's systems, information or data is revoked
  - all passes and / or equipment issued by the Trust are returned
  - any Trust information or data held on the systems of the Third-party shall be deleted or destroyed, in accordance with the Records Retention Policy.

In the case where a contract has been offered and accepted by a third party without the Commercial Team being made aware, the relevant Executive Director will contact the Commercial Team as soon as feasibly possible to ensure that the relevant contractual undertakings can be established.

4. TRAINING

4.1 The information Governance Team are responsible for training being provided to The Executive Leadership Team, Senior Information Risk Owners, The Caldicott Guardian, Information Asset Owners, Information Governance staff and Procurement / Commercial staff . This training will be undertaken as part of the individual's induction and as part of annual refresher training; individuals will be trained and assessed against the tasks outlined within the policy.

5. EQUALITY IMPACT ASSESSMENT

5.1 Solent NHS Trust is committed to treating people fairly and equitably regardless of their age, disability, gender, reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

5.2 An equality and human rights impact assessment has been carried out for the purpose of this policy and no significant issues have been identified (See Appendix A).

6. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

6.1 As a minimum the following will be monitored to provide assurance that this policy is being adhered to and the Trust's legal obligations are met:

- All new contracts with third-party suppliers have been assessed against Data Protection Security standards and where applicable a Data Protection Impact Assessment has been conducted.
- All existing contracts requiring renewal are assessed or re-assessed against Data Protection Security standards and where applicable a Data Protection Impact Assessment has been conducted.
- Any existing systems or processing agreements with third-party suppliers, where the processing is considered high risk by the Trust's Data Protection Officer, are to be assessed against Data Protection Security standards and a Data Protection Impact Assessment has been conducted

6.2 The above will be assessed at least annually, by the Information Governance Team in accordance with the Trust's annual submission of the Data Security and Protection Toolkit.

6.3 The above may also be subject to both internal audit assessment and independent audit assessment conducted by NHS Digital.

6.4 Failure to adhere to this policy will initiate the Improving and Managing Conduct Policy and captured on the Trust's Risk Register.

7. REVIEW

7.1 This document may be reviewed at any time at the request of either staff side or management but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

8. REFERENCES AND LINKS TO OTHER DOCUMENTS

8.1 This section provides the research and evidence that were used to assist with the development of this Policy. It is recommended that this Policy should be read and used in conjunction with other relevant documents detailed below (as applicable).

- Data Protection Act 2018 / General Data Protection Regulations 2016
- Data Security & Protection Toolkit
- Data Protection Compliance Policy

9. GLOSSARY

Abbreviation	Full Name
DPO	Data Protection Officer
ICT	Information and Communication Technology

Appendix A: Equality Impact Assessment

Step 1: Scoping and Identifying the Aims		
Service Line / Department	Information Governance	
Title of Change:	Third Party Suppliers Data Protection & Security Assurance Policy	
What are you completing this EIA for? (Please select):	Policy	*(If other please specify here)*
What are the main aims / objectives of the changes	To ensure that the Trust and its contractors meet their legal requirements, as outlined by the Data Protection Legislation, with regards to the procurement and contracting of services, involving the processing of Personally Identifiable Data	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Not applicable	Action to address negative impact: *(e.g. adjustment to the policy)*
Sex			x	
Gender reassignment			x	
Disability			X	
Age			X	
Sexual Orientation			X	
Pregnancy and maternity			X	
Marriage and civil partnership			X	
Religion or belief			X	
Race			x	

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	Please select	
Have you taken into consideration any regulations, professional standards?	Please select	

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation if no action taken?	Low	Medium	High
	■	☐	☐
What action needs to be taken to reduce or eliminate the negative impact?	N/A		
Who will be responsible for monitoring and regular review of the document / policy?	Data Protection Officer		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	*Sadie Bell*	*Date:*	*09/05/2022*