INFORMATION GOVERNANCE THIRD PARTY POLICY

(IG requirements re organisations or Individuals Supplying Goods, Services or Consultancy to the Isle of Wight NHS Trust)

Policy Type	Information Governance
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Information Governance Lead Officer
Next Author Review Date	01 October 2022
Approving Body	Policy Management Sub-Committee
Version No.	3.0
Policy Valid from date	01 March 2019
Policy Valid to date:	31 March 2023

'During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Advisory Group and where necessary other relevant Oversight Groups'

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
Oct 13	0.3		Foundation Trust Programme Director / Company Secretary	Amended section on monitoring compliance	
11 Jun 14	0.4		Foundation Trust Programme Director / Company Secretary	Reviewed at	Information Steering Group
01 Jul 14	0.4		Foundation Trust Programme Director / Company Secretary	Ratified on voting buttons by	Information Steering Group
20 Aug 14	0.4		Foundation Trust Programme Director / Company Secretary	Ratified at	Risk Management Committee
16 Sep 14	0.4		Foundation Trust Programme Director / Company Secretary	Policy review Minor changes needed to 3.3, 12.3 & App A	
18 Nov 14	0.4		Foundation Trust Programme Director / Company Secretary	Ratified at	Policy Management Group
24 Nov 14	1	24 Nov 14	Foundation Trust Programme Director / Company Secretary	Approved at	Trust Executive Committee
15 Mar 18	1.1		Deputy Chief Executive	Policy reviewed and updated Governance Structure to be ratified	Information Governance Sub-Committee
8 May 18	1.1		Deputy Chief Executive	Approved at	Policy Management Sub-Committee
25 May 18	1.1		Deputy Chief Executive	Voting buttons following GDPR updates	Information Governance Sub-Committee
13 June 18	2.0	13 June 18	Deputy Chief Executive	Approved at	Policy Management Sub-Committee
Feb 2019	2.1		Director of Finance, Estates and IM&T	Policy reviewed and updated	
12 Mar 19	3.0	12 Mar 19	Director of Finance, Estates and IM&T	Policy approved subject to endorsement at IGSC	Policy management Sub-Committee
14 Mar 19	2.1		Director of Finance, Estates and IM&T	Endorsed at	Information Governance Sub-Committee
July 2020	2.2		Director of Finance, Estates and IM&T	Review following ICO audit	
30/07/2020	2.2		Director of Finance, Estates and IM&T	Contents agreed via voting buttons and approval by Chair at	Information Governance Sub-Committee
30/07/2020	3.0	30 July 2020	Director of Finance, Estates and IM&T	Approved at	Policy Management Sub-Committee
29 Jan 21	3.0		Quality & Performance committee	12 month blanket policy extension due to covid 19 applied with author review date set 180 days prior to Valid to Date.	Quality & Performance committee
22 April 2021	3.0	30 July 2020	Director of Finance, Estates and IM&T	Extended policy uploaded and linked back	Corporate Governance

NB This policy relates to the Isle of Wight NHS Trust hereafter referred to as the Trust

Contents

1 Executive Summary

This policy provides guidance on why the Trust requires an Information Governance Third Party Policy and details the main benefits to the organisation to ensure its legal requirements and provide a comprehensive guidance document on the Trust's expectations to any staff who contribute in any capacity, to the governance of Information.

This policy provides details of:

- What constitutes a Third Party
- The agreement that a Third party subscribes to when working on or behalf of the Trust
- A confidentiality agreement for contracted staff

2 Introduction

The Trust is committed to protecting the information it holds and safeguarding all activities carried out both on and off IOW NHS Trust's premises by Third Parties in accordance with its legal duty as a data controller under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulations (GDPR).

The importance of robust Information Governance has risen rapidly in recent years following the ongoing concerns related to security and confidentiality of Public Sector data and the increased enforcement powers assigned to the Information Commissioner's Office.

It is paramount that all organisations and individuals protect the Trust's information assets in line with policy and standards and European and UK legislation. This Policy has been produced in recognition of the need to provide clear and unambiguous confidentiality and information security requirements to Third Parties who may process information on behalf of the Trust or potentially have access to the Trust's information assets and must be adhered to by the Trust when engaging Third Parties. These requirements are reflected within the NHS Data Security Protection Toolkit (DSPT).

This Policy should be read in conjunction with the Information Governance Policy including the Management of Information Risks.

Any questions of interpretation within this policy must be raised immediately with the Information Governance Lead Officer (IGLO) or delegated officer.

3 Definitions

For a full list of definitions please refer to the Trust's Information Governance Management Framework.

The following definitions have been adopted by the Trust:-

3.1 Data Subject

Data subject is defined as an individual who is the subject of personal data and relates to whom the particular personal data/information is about.

3.2 Third Party

An organisation or person, who supply goods, services and / or consultancy to the Trust and who will or are likely to have access to Personal Confidential Data as part of the Trust's information assets. Information assets may be accessed within the Trust's premises or external to the Trust premises

4 Scope

This Policy applies to organisations or individuals (hereafter referred to as the Third Party*****) who supply goods, services and / or consultancy to the Trust and who will or are likely to have access to the Trust's information assets which including Personal Confidential Data. Information assets may be accessed within the Trusts premises or external to the Trust premises.

****Third Party also extends to any person employed or engaged by the Third Party in connection with the contract e.g. sub-contractors, agents.***

This Policy also applies to those individuals or organisations that perform voluntary / casual work within the Trust or carry out research / investigatory / project work on behalf of or within the Trust. In such cases the arrangement / agreement to carry out the work will constitute a contract and the parties will be bound by the terms of the contract agreement and especially the Information Governance conditions specified in this policy, which must be reflected in those contracts

Third Parties may include, but are not limited to:

- Hardware and Software maintenance and support staff
- Cleaning, catering, security and other outsourced support services
- Temporary workers and/or Agency Staff
- Non – NHS employed staff working in the local Community
- Nursing and Residential Homes
- Independent Pharmacies
- External IT support staff
- Suppliers of any type of goods, systems or services
- Consultants, External Contractors, Medical Agencies, Project Staff
- External trainers
- Any other party not directly employed by the Trust

5 Purpose

The purpose of this policy is to ensure that every member of staff who has a contracting role / obligation or engages a third party within their remit recognises the IG risks associated with external contractors using/having access to Trust Information.Third Parties must be made

aware through this policy of their personal responsibility for ensuring that all associated risks through this process are recognised and mitigated accordingly.

6 Roles and Responsibilities

For a full list of roles and responsibilities please refer to the Trusts IG Management Framework.

6.1 Chief Executive Officer (CEO)

Overall responsibility for Information Governance within the Trust rests with the Chief Executive, who as the Accountable Officer must ensure that the right policies, procedures and systems are in place and kept under review.

6.2 Senior Information Risk Owner (SIRO) / Director of Governance and Risk

The SIRO is responsible for ensuring that the supporting Information Risk Management structure of Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) is in place to facilitate the implementation of third party agreements and contracts. ;

6.3 Caldicott Guardian (CG)

The Caldicott Guardian is responsible for ensuring that any risks to personal confidential data from third parties are mitigated through this policy.

6.4 Information Governance Lead Officer (IGLO)/Data Protection Officer (DPO)

The DPO assists with monitoring internal compliance, informing and advising on DPA obligations, Data Protection Impact Assessments (DPIAs) and contracts. The DPO also investigates personal data breaches/security breaches that may have arisen as a result of a contract or third party agreement. This role is assigned to the Information Governance Lead Officer.

6.5 Information Asset Owners (IAOs)

IAOs are responsible for ensuring that any third party contract requirements are identified and implemented as required and ensure that any risks are mitigated.

6.6 Information Asset Administrators (IAAs)

IAAs are responsible for supporting the IAO in discharging their duties under this policy.

7 Policy detail/Course of Action

7.1 Trust must:

- Ensure that where a Third Party is to be engaged, an appropriate Data Protection Impact Assessment (DPIA) in accordance with the Trust DPIA Framework Guidance is carried where appropriate to identify the scope of any information required for the purpose of the contract and the legal basis for sharing the information. The DPIA template is included within the DPIA Framework Guidance (which can be found on the Trust intranet) or can be obtained from the IG Team.

- Ensure that, where required (as identified from the DPIA) that a Data Sharing Agreement (DSA) is also completed.

- Ensure that the transfer of any data is risk assessed, justified and not excessive for the purpose of the data required / requested.

- For services engaged by the Trust's Estate Management ensure that a Site Rules for Contractors agreement is provided to all Third Party contractors before starting work on the Trusts sites.

- Ensure copies of the signed agreement are held by both the Third Party and the Information Asset Owner (IAO).for Estates.
- Ensure that any confidential information communicated to the Third Party is completed securely and in accordance with Trust policy i.e. encryption for all portable media / electronic transfer of personal confidential data and returned to the Trust premises or securely disposed of at the end of the contract in accordance with the agreed terms and conditions in the Contract and in line with the Records Management Code of Practice for Health and Social Care 2016.

- Report immediately, any suspected or actual information security breaches / personal data breaches involving the third party through the Trust incident reporting process (please refer to the Trusts Risk Management Policy)

7.2 Third Parties must:

- Treat all information received from the Trust as confidential; which may be derived from or be obtained in the course of any contract, agreement or any other arrangement between the Trust and those third parties; or which may come into the possession of the Third Party or an employee, servant, agent or sub-contractor of the Third Party as a result or in connection with the contract; and
- Provide all necessary precautions to ensure that all such information is treated as confidential by the Third Party, his employees, servants, agents or sub-contractors; and
- Ensure that he, his employees, servants, agents and sub-contractors are aware of the provisions of the DPA 2018 and General Data Protection Regulations.
- Ensure that they are registered accordingly under the DPA and that any personal information obtained from the Trust shall not be disclosed or used in any unlawful manner; and
- Indemnify the Trust against any loss arising under the DPA caused by himself, his employees, servants, agents or sub-contractors.

7.3 Contracts:

All third parties that engage with the Trust must have in place a robust contract. Healthcare contracts must be processed through the Trust's contracting team. The NHS Standard Contract is mandated by NHS England for use by commissioners for all contracts for healthcare services other than primary care. The NHS Standard contract must therefore be utilised wherever possible due to the fact that the terms and conditions within the standard contract contain all the necessary IG and confidentiality clauses. For any contract that does not utilise the NHS Standard Contract, a separate confidentiality agreement will need to be considered and if necessary advice in relation to any agreement sought from the Information Governance team prior to any contract being issued.

8 Consultation

The review of this policy has been in consultation with the SIRO and IGSC membership (which includes IAOs) who are responsible for supporting the SIRO in delivery of the Information Risk Management agenda. It has also been reviewed by the Trust contracts team.

9 Training

This Information Governance Third Party Policy does not have a mandatory training requirement or any other training needs however mandatory Data Security Awareness training is an annual requirement for all staff.

10 Monitoring Compliance and Effectiveness

The Third Party Policy supports the annual DSP toolkit submission; this provides the means by which the Trust assesses their compliance with current legislation, government policy and national guidance.

As part of the DSPT there is an annual requirement within the overall action plan for all formal contractual arrangements with contractors and support organisations to be reviewed. This ensures that they remain effective with any contract clauses updated as necessary. In addition to the national submission all DSPT related reports are received by the Information Governance Sub Committee (IGSC).

The Care Quality Commission (CQC) also uses the DSPT as part of the standard to audit NHS organisations against the Essential Standards of Quality and Safety.

Any IG incidents in relation to any contracts with third parties are reportable in accordance with the Trust Incident Management System reporting standards and SI policy. All IG incidents are monitored and reviewed as a regular agenda item at IGSC.

11 Links to other Organisational Documents

- Records Management Policy
- Confidentiality NHS - Code of Practice
- Incident Management Policy

- Serious Incidents Requiring Investigation (SIRI)Guidance
- Guide to the Notification of Data Security and Protection Incidents
- Being Open Policy and Process
- Information Governance including the Management of Information Risks Policy
- IOW NHS Trust's Procurement Strategy
- Missing or Misplaced Clinical Records Procedure
- NHS Employment Check Standard
- DPIA Framework Guidance and DPIA Template
- Data Sharing Procedure

12 References

- Public Records Act 1958 and 1967
- Access to Health Records Act 1990
- Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2016
- Caldicott Review of Patient Identifiable Information 1997; Caldicott 2 Review 2013
- National Data Guardian review of Data Security Consent and Opt Outs 2016
- Department of Health: Confidentiality Code of Practice 2003
- NHS Digital Data Security Protection Toolkit
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Re-Use of Public Sector Information Regulations 2005

13 Appendices

Appendix A Financial and Resourcing Impact Assessment on Policy Implementation

Appendix B Equality Impact Assessment (EIA) Screening Tool

Appendix A

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	**Information Governance Third Party Policy**

Totals	**WTE**	**Recurring £**	**Non-Recurring £**
Manpower Costs	N/A	None	None
Training Staff	See below	None	None
Equipment & Provision of resources	N/A	None	None

Summary of Impact:

Risk Management Issues:

Benefits / Savings to the organisation:

Equality Impact Assessment

- Has this been appropriately carried out? **YES**/NO
- Are there any reported equality issues? YES**/NO**

If "YES" please specify:

Use additional sheets if necessary.

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	**WTE**	**Recurring £**	**Non-Recurring £**
Operational running costs		N/A	N/A
Totals:		None	None

Staff Training Impact	**Recurring £**	**Non-Recurring £**
Part of Information Governance mandatory training for all staff.	To be absorbed	
Totals:	None	None

Equipment and Provision of Resources	Recurring £ *	Non-Recurring £ *
Accommodation / facilities needed	N/A	N/A
Building alterations (extensions/new)	N/A	N/A
IT Hardware / software / licences	N/A	N/A
Medical equipment	N/A	N/A
Stationery / publicity	N/A	N/A
Travel costs	N/A	N/A
Utilities e.g. telephones	N/A	N/A
Process change	N/A	N/A
Rolling replacement of equipment	N/A	N/A
Equipment maintenance	N/A	N/A
Marketing – booklets/posters/handouts, etc.	N/A	N/A
Totals:	**None**	**None**

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	
Signature & date of financial accountant:	
Funding / costs have been agreed and are in place:	
Signature of appropriate Executive or Associate Director:	

Appendix B

Equality Impact Assessment (EIA) Screening Tool

Document Title:	Information Governance Third Party Policy
Purpose of document	To ensure that all staff are aware of their contracting obligations within their remit
Target Audience	All staff
Person or Committee undertaken the Equality Impact Assessment	Information Governance Lead Officer

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?

If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.

If yes please detail underneath in relevant section and provide priority rating and determine if full EIA is required.

		Positive Impact	**Negative Impact**	**Reasons**
Gender	Men	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Women	*NA*	*NA*	*Sets out how the Trust complies with the law*
Race	Asian or Asian British People	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Black or Black British People	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Chinese people	*NA*	*NA*	*Sets out how the Trust complies with the law*
	People of Mixed Race	*NA*	*NA*	*Sets out how the Trust complies with the law*
	White people (including Irish people)	*NA*	*NA*	*Sets out how the Trust complies with the law*

	People with Physical Disabilities, Learning Disabilities or Mental Health Issues	*NA*	*NA*	*Sets out how the Trust complies with the law*
Sexual Orientation	Transgender	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Lesbian, Gay men and bisexual	*NA*	*NA*	*Sets out how the Trust complies with the law*
Age	Children	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Older People (60+)	*NA*	*NA*	*Sets out how the Trust complies with the law*
	Younger People (17 to 25 yrs.)	*NA*	*NA*	*Sets out how the Trust complies with the law*
Faith Group		*NA*	*NA*	*Sets out how the Trust complies with the law*
Pregnancy & Maternity		*NA*	*NA*	*Sets out how the Trust complies with the law*
Equal Opportunities and/or improved relations		*NA*	*NA*	*Sets out how the Trust complies with the law*

Notes:

Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3. Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	**NO**
Legal (it is not discriminatory under anti-discriminatory law)		N/A	N/A
Intended		N/A	N/A

If the negative impact is possibly discriminatory and not intended and/or of high impact then please complete a thorough assessment after completing the rest of this form.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:
N/A

3.2 Could you improve the strategy, function or policy positive impact? Explain how below:	
N/A	
3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?	
Scheduled for Full Impact Assessment	Date: N/A
Name of persons/group completing the full assessment.	N/A
Date Initial Screening completed	