

# Information Risk Policy

**Controlled document**

**This document is uncontrolled when downloaded or printed**

<b>Author(s) Owner(s)</b>	Author: Gill Richards, Head of Information Governance Owner: Shelley Ramtuhul, Director of Governance/Senior Information Risk Owner (SIRO)
<b>Version No.</b>	Version 1.4
<b>Approval Date</b>	June 2023
<b>Review Date</b>	June 2026

<b>Document Details</b>		
Title	<b>Information Risk Policy</b>	
Trust Ref No	1341-36341	
Local Ref (optional)	1.4	
Main points the document covers	Information Asset Owners responsibilities, training, risk assessment. Risk assessment, management and appetite	
Who is the document aimed at?	All staff (including non-employed workers)	
Author	Head of Information Governance	
<b>Approval process</b>		
Who has been consulted in the development of this policy?	Members of the Data Security and Protection Assurance Group (DSPAG), Information Governance Team.	
Approved by (Committee/Director)	Audit Committee, Chaired by Non-Executive Director	
Approval Date	16 June 2023	
Initial Equality Impact Screening	Yes	
Full Equality Impact Assessment	No	
Lead Director	Director of Governance	
Category	General	
Sub Category	Information Governance	
Review date	16 June 2026	
<b>Distribution</b>		
Who this policy will be distributed to	Publication on the Trust Websites, all staff, IAOs, IAAs, Information Governance Team.	
Method	Websites, Trust Newsletter	
Keywords		
<b>Document Links</b>		
Required by CQC	Yes – Well Led	
Other		
<b>Amendments History</b>		
No	Date	Amendment
1		Appendix C & D updated Authors name updated Update to include GDPR/DPA2018
2	December 2021	The whole document was reviewed by a consultancy and then finalised by the IG Manager
3	July 2022	Update to IT Service Manager description
4	October 2022	Update Owner - Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
5	March 2023	Amended IG Manager to Head of IG. Updated Safe Haven role to function. Updated IAO role. Updated role of Information Risk Manager to include assigned to Head of

---

		IG. Included clear IAO responsibilities as Appendix C. Updated Risk Review procedure Appendix D.
--	--	---

---

## CONTENTS

1. Introduction.....	4
2. Purpose.....	4
3. Scope and Applicability .....	5
4. Related Documents.....	5
5. Policy Statement .....	6
6. Responsibilities .....	8
7. Audits and Assessments .....	11
8. Data Losses and Confidentiality/Security Breaches .....	11
9. Training .....	12
10. Review and Monitoring.....	12
11. Information Standards .....	12
12. Glossary .....	13
Appendix A: Legal and Regulatory Requirements .....	14
Appendix B: Examples of Information Assets .....	15
Appendix C: Information Asset Owner Responsibilities .....	16
Appendix D: Risk Review Procedure for Information Assets .....	18

---

## 1. Introduction

- 1.1 This policy relates to information risk for Shropshire Community Health NHS Trust (hereafter referred to as the Trust).
- 1.2 The Board recognises information risk is inherent in the provision of healthcare and its services. Understanding and working within the Trust's Information Risk Appetite is at the core of protecting the information which drives and supports its business.
- 1.3 The Trust is highly reliant on information that is captured, stored, processed and delivered by information systems and their associated communication facilities.
- 1.4 Such information plays a vital role in supporting businesses processes and patient services, in contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.
- 1.5 Accordingly, the information and the enabling technologies are important assets that will be protected to the level commensurate with their value to the Trust.
- 1.6 The key requirement of this policy is for information risk to be managed in a robust way within work areas. Information risk must not be seen as something that is the sole responsibility of IT or Information Governance staff and is part of everyday practice by all staff members.

## 2. Purpose

- 2.1 This policy defines how the Trust will manage information risk and how effectiveness will be assessed and measured e.g. through the Information Risk Appetite framework

*This policy provides the framework to allow an information risk appetite for different information assets to be defined and is the starting point that dictates how to protect and safely exploit information.*

- 2.2 It is the policy of the Trust to ensure that the approach to information risk management:
  - Takes full advantage of existing authority and responsibility structures where these are fit for this purpose
  - Associated tasks with appropriate management levels
  - Avoids unnecessary impacts on day-to-day business
  - Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner
  - Supports a culture which encourages well informed decision making through a focus on proactive rather than reactive Information Risk Management.

### **3. Scope and Applicability**

- 3.1 This policy sets out the Trust's approach to risk as it relates to all information obtained and processed within the Trust held in electronic, paper-based and other formats, whether stored in automated or manual systems, relating (but not limited) to:
- patient/ client / service user information
  - staff and personnel information
  - Trust business, commercial and operational information
  - Research, audit and reporting information.
- 3.2 This policy is to ensure that all staff are aware of their individual responsibilities in relation to the management of information risk. Legal and Regulatory Requirements are listed in Appendix A.
- 3.3 This policy applies to all Trust staff (including temporary workers, locums and staff seconded or contracted from other organisations) and parties authorised by the Trust together with their staff (including temporary workers, locums and staff seconded or contracted from other organisations).

### **4. Related Documents**

- 4.1 The information risk policy should be read in conjunction with the Trust's overall Risk Management Strategy and Risk Assessment Code of Practice; information risk need not be managed separately from other business risks but should be considered a fundamental component of effective information governance.
- 4.2 The following Shropshire Community Health NHS Trust documents contain information that relate to this policy:
- Data Protection Policy
  - Information Quality Assurance Policy
  - Information Security Policy
  - Records and Document Management Policy
  - Risk Management Policy
  - Risk Assessment Code of Practice
  - Incident Reporting Policy
  - Incident Reporting on DATIX
  - The Board's Information Risk Appetite Statement
  - Whistleblowing Policy and Procedure.

---

## 5. Policy Statement

### Contextualising Risk

- 5.1 The definition of risk in this context provided by NHS Digital is “The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood”. Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk.
- 5.2 Full descriptive definitions of risk management and the risk management process, drawn from AS/NZS 4360:1999, are described in the Trust’s Risk Management Strategy.
- 5.3 The likelihood and impact of the risks facing the Trust depend on how vulnerable the Trust is to threats. Threats can be categorised as either external or internal. Although the mechanisms of these threats are different, both are equally capable of causing damage to the Trust, its patients, clients, its partners and staff.
- 5.4 External threats may include:
- state-sponsored Cyber activities: disruption, denial of service, malware attack, etc.
  - Serious Organised Crime
  - online political activists (sometimes referred to as “hacktivists”)
  - environmental (extreme weather events)
  - industrial espionage and competitor threats, including commercial interests.
- 5.5 Internal threats may include malicious insiders and non-malicious insiders, caused by:
- inadequate IT design
  - lack of physical / IT controls
  - lack of procedural controls, training and /or awareness
  - malicious motivations e.g. financial gain, disgruntled employee.

### Information Assets

- 5.6 An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the Trust. Information Assets come in many shapes and forms, and an illustrative list is given in Appendix B. It is the responsibility of Information Asset Owners to identify new information assets and ensure they are recorded on the Information Asset Register managed by the Information Governance Team.
- 5.7 Irrespective, the nature of the information assets themselves, they all have one or more of the following characteristics:
- They are recognised to be of value to the Trust

- They are not easily replaceable without cost, skill, time, resources or a combination
- Their loss would cause reputational damage to the Trust
- Their data classification would normally be 'confidential'
- The asset is maintained by people working in a consistent and cooperative manner.

5.8 An Information Asset increases in value according to the amount of analysis it performs converting low level Information into more refined Information.

### **Business-Critical Information Assets**

5.9 The Trust shall ensure that all Business-Critical Information Assets are individually identified, recorded and monitored in accordance with this policy.

A Business-Critical Information Asset is defined as follows:

- A body of knowledge / information that, if access to it were denied (lost, unavailable, compromised or stolen) the business would cease to function / operate/realise its business outcomes for a period of time; and/or,
- An Information Asset that would seriously undermine the ability of the Trust to fulfil its obligations as part of UK Critical National Infrastructure, if a Third Party Organisation were to obtain it.

### **Information Risk Appetite**

5.10 Information Risk Appetite is best expressed as a series of boundaries, appropriately authorised by senior management, which give each level of the Trust clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it.

5.11 Her Majesty's Treasury (HMT) advocates the use of five categories of Risk Appetite. Within this framework, an Information Asset will have a different Information Risk Appetite applied to it, depending on the sensitivity/value of that asset. The five categories are outlined below:

- **Adverse** - Avoidance of risk and uncertainty is a key Trust objective.
- **Minimalist** - Preference for ultra-safe business delivery options that have a low degree of residual risk.
- **Cautious** – Preference for the safe delivery options that have a low degree of residual risk.
- **Open** - Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable reward (and value for money etc.).
- **Hungry** - Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.



## Risk Appetite Statement

- 5.12 The Trust's SIRO shall utilise the Information Risk Appetite framework to agree and set risk tolerances with the IAOs of each business area. If for any reason operational requirements require a specific unit or business area to reduce the agreed level of Information Risk Appetite, then a risk balance case shall be presented to the SIRO or, where applicable, the Board for formal approval, and the decision recorded.
- 5.13 Likewise, if the impact of a risk has the potential to extend beyond the unit or business area across the Trust more widely, (e.g. reputational risk), IAOs must consult with the Trust's SIRO to determine the way ahead.

Trust Statement on Risk Appetite is given below. Full details are set out in the Risk Management Strategy/Policy.

'Shropshire Community Health NHS Trust will seek to prevent, mitigate, cope with, transfer, accept and/or reject risks which have the potential to;

- Adversely impact reputation of the Trust
- Expose patients, staff, visitors and stakeholders to harm
- Limit ability to deliver strategic and operational priorities
- Cause significant financial consequences which would jeopardise ability to deliver and carry out mandated priorities
- Cause non-compliance with the law and regulation
- Result in barriers to active engagement with system partners, research and innovation being embedded into 'shropcom culture'

*This policy provides the framework to allow an information risk appetite for different information assets to be defined and is the starting point that dictates how to protect and safely exploit information.*

## Controls

- 5.14 Controls are mechanisms to mitigate the risk or address any vulnerabilities. These may be procedural or physical as well as technical. Information Assets towards which the Trust has an 'Averse' Information Risk Appetite will require much stricter controls than those where an 'Open' or 'Hungry' Information Risk Appetite is allocated.

## 6. Responsibilities

- 6.1 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

---

Under the data protection legislation, the Trust is required to demonstrate that it has an information governance framework supported by the following roles:

- 6.2 The **Board** provides leadership on the management of risk and ensures the approach to risk management is consistently applied as well as determining the information risk appetite for the Trust. The Board is also responsible for setting the Trust's Risk Appetite regarding information security.
- 6.3 The **Senior Information Risk Owner (SIRO)** is the Board's executive level delegate responsible for risk management including oversight of data protection and other aspects of information governance. The role of the SIRO is to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board, including internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control (SIC) with regards to information risk. The SIRO will advise the Chief Executive and the Board on information risk management strategies, provide periodic reports and briefing on risk management assurance and ensure that key risks are appropriately logged on the corporate risk register.
- 6.4 The **Chief Executive** is the Accountable Officer and has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation. They have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. The organisation will set out a line of accountability, responsibility and direction in accordance with the guidance set out in the Data Security and Protection Toolkit (DSPT) Standard 1 Personal Confidential Data, example diagram given below.
- 6.5 The **Chief Information Officer (CIO)** is an executive within the organisation that oversees the operation of the information technology department and consults with other personnel on technology-related needs and purchasing decisions. The CIO is the Head of Digital Services.
- 6.6 The **Caldicott Guardian (CG)** has responsibility for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. For any patient confidentiality issues the first point of contact should be the CG. The CG is also the designated **Privacy Officer**.
- 6.7 The **Chief Clinical Information Officer (CCIO)** is an executive within the organisation who is involved in change management, ensuring clinical adoption and engagement in the use of technology, supporting clinical process redesign in a digital world, providing clinical focus to ICT projects that will ensure the needs of the business are met with regards to patient care. The CCIO is the Medical Director/Caldicott Guardian.
- 6.8 The **Data Protection Officer (DPO)** has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for

---

escalation as appropriate. The DPO is responsible for challenging and advising the Board on data protection to ensure that the Trust remains compliant.

- 6.9 The role of the **Information Asset Owner (IAO)** will be assigned to staff that hold the position of Deputy/Associate Director, Head of Department, Service Delivery Group Manager. The IAOs will be accountable to the Senior Information Risk Owner (SIRO); and will have delegated responsibility from the SIRO to oversee and support the information risk management framework within their respective areas. The role will support the SIRO in fostering a culture that values, protects and uses information for the benefit of patients, service users, employees and the Trust as whole. Full responsibilities listed in Appendix C.
- 6.10 The Information Asset Owner may nominate an **Information Asset Administrator (IAA)** and delegate the day-to-day responsibility of the information asset. The Information Asset Owner will nominate an appropriate person to undertake the role of **Data Protection Liaison Officer (DPLLO)**.
- 6.10 **Data Protection Liaison Officers (DPLLO)** is responsible for providing administrative support to staff within the respective services/departments in the disclosure of personal data under the Data Protection legislation.
- 6.11 The **Information Governance Manager** is responsible for the day-to-day operational monitoring and managing of information governance and information handling.
- 6.12 The **IT Services Manager** is responsible for the day-to-day management and operation of the corporate network infrastructure including the secure operation of the network, devices, connections, monitoring, protection and controls.
- 6.13 A **Safe Haven function** will be established in all services, teams and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information; such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g. Trust premises or a virtual location e.g. MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.
- 6.14 The **Information Risk Manager** is responsible for providing support to staff and managers who are responsible for information assets. They will provide support to the relevant groups and committees, including risk registers and monitoring service delivery risks. The role of the Information Risk Manager will be undertaken by the Head of Information Governance.

- 6.15 The **Freedom of Information Manager** to ensure that the Trust complies with the Freedom of Information Act 2000 in processing Freedom of Information requests and the maintenance of a Publication Scheme. This role will manage the need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. Advising the organisation with regards to deciding whether the information can be released without infringing the UK GDPR and DPA 2018 data protection principles.
- 6.16 **All Line Managers** are responsible for ensuring that staff with responsibilities set out in this policy can undertake the role sufficiently, including training, to meet the organisation's obligations under the Data Protection legislation.
- 6.17 **All Staff** are responsible for upholding Data Protection requirements, including identifying and managing risk and understanding/complying with relevant policies and procedures for handling personal data appropriate to their role. Staff must immediately report any event or breach affecting personal data held by the organisation to their Line Manager.

## 7. Audits and Assessments

7.1 In accordance with NHS guidance comply with the audit and assessment requirements and document the findings and outcomes.

7.2 IAOs and staff involved in procuring new systems and technology must conduct and complete appropriate assessments in accordance with NHSX guidance here: [Digital Technology Assessment Criteria \(DTAC\) - Key tools and information - NHS Transformation Directorate \(nhsx.nhs.uk\)](#).

7.3 For new products the assessment should be undertaken in conjunction with the Procurement Lead, IAO and the service/department/team manager using the [DTAC Form](#).

7.4 The DTAC form must be formally approved and signed off and then included as part of the IAR record.

## 8. Data Losses and Confidentiality/Security Breaches

8.1 All incidents that constitute a loss of information, vulnerability, threat or serious incident which could potentially lead to a breach of patient confidentiality must be reported, in accordance with the Trust's Incident Reporting Policy and Incident Reporting on Datix; by the IAO directly to the Trust Information Risk Manager, DPO, the Caldicott Guardian and the SIRO.

- 
- 8.2 All incidents that constitute a loss of information which could potentially lead to a breach of staff confidentiality must be reported by the IAO directly to the Trust DPO and the SIRO.
  - 8.3 The incident reporting process is set out in the Trust's Incident Reporting Policy and Incident Reporting on Datix; and the Trust's Information Security Policy.
  - 8.4 Near misses relating to Personally Identifiable Information, Personal Confidential Data (PID/PCD) should be reported by the IAO in accordance with the Trust's Incident Reporting Policy and Incident Reporting on Datix; and to the SIRO.

## **9. Training**

- 9.1 All new staff (employed and non-employed) will be given Cyber Security and Information Governance training as part of their corporate induction training.
- 9.2 The Trust will provide Cyber Security and Information Governance training to all staff as part of its annual mandatory training programme and attendance will be recorded and monitored (if appropriate).
- 9.3 The Trust will provide appropriate role specific Cyber Security and Information Governance training for key roles following training needs analysis.
- 9.4 The Trust will ensure that their staff are aware of its policies and requirements regarding Information Risk and appropriate training arrangements will be made available.
- 9.5 Links between Information Risk and other Information Governance requirements will be clarified for staff.

## **10. Review and Monitoring**

- 10.1 This policy will be reviewed annually, as required by the Head of Information Governance, or in response to changes due to security incidents, changes to the Trust's technical infrastructure, legislative amendments, or updates made to the Data Security and Protection Toolkit (DSPT).
- 10.2 The Data Security and Protection Assurance Group will review incidents for trends or patterns and impacts on controls in place and provide a commentary for an annual risk assurance report.
- 10.3 Any breach of or refusal to comply with this policy will lead to disciplinary action in accordance with the Trusts' Human Resource policy framework available on the Trust's website.

## **11. Information Standards**

- 11.1 Each provider should ensure all systems are compliant with all relevant information standards published by NHS Digital on the Information Standards website and that their systems suppliers have implemented all applicable standards and are similarly compliant.

- 11.2 National definitions and guidance support the sharing, exchange and comparison of information across the NHS and other care providers. Common definitions, known as information standards, are used for commissioning purposes, to support comparative data analysis, for the preparation of performance tables, for data returns to the Department of Health and Social Care and also support clinical messages, such as those used for pathology and radiology.
- 11.3 National information standards should not just be seen as supporting the collection of data on a consistent basis throughout the NHS and other care providers. They also have an important role in supporting the flow and quality of information used, so that health and care professionals are presented with the relevant information where and when it is required to provide effective care and treatment to service users.
- 11.4 Organisations should ensure that:
- Electronic systems have built in data quality checks which are conformant with, or map to national Data Standards (where these exist);
  - For the relevant service user information systems, where national data standard definitions and values exist:
    - values on the key systems match the national standard definitions;
    - no other values are used unless these are mapped explicitly for central returns;
    - the number and combination of alpha/numeric digits within a code match the format of the NHS Data Dictionary and the code conforms or maps to a nationally determined coding structure (where these exist).
- 11.3 Organisations should also have policies / procedures to ensure:
- Validation routines are used routinely on data entry to assure completeness and validity of datasets, both those used locally and for central returns;
  - Standard definitions used in data schemas on key systems, checking all entries on the schema relating to these definitions against national definitions and codes;
  - Monitoring in place to identify and resolve duplicate records.

## 12. Glossary

<b>Term / Abbreviation</b>	<b>Explanation / Definition</b>
NHSD	NHS Digital (Successor to HSCIC)
IAA	Information Asset Administrator
SA	System Administrator
DSPT	Data Security and Protection Toolkit (DSPT)
SCHT	Shropshire Community Health NHS Trust
PID	Personally Identifiable Data
PCD	Personal Confidential Data

## Appendix A: Legal and Regulatory Requirements

Legal and Regulatory Requirements applicable to the management of information risk:

<b>Details</b>	
Access to Health Records Act	1990
Communications Act	2003
Computer Misuse Act	1990
Confidentiality NHS Code of Practice	
UK General Data Protection Regulation (UK GDPR)	2018
Data Protection Act	2018
Electronic Communications Act	2000
Freedom of Information Act	2000
Human Rights Act	1998
NHS Information Governance Codes of Practice	
Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2001).	
Risk Assessment Code of Practice	

## Appendix B: Examples of Information Assets

<b>Personal Information Content</b>	<b>Software</b>
Databases and data files Back-up and archive data Audit data Paper records and Paper reports Patient information and data Employee records and data such as: Human Resources information and payroll for staff, contractors and sub-contractors.	Applications and System Software Data encryption utilities Development and Maintenance tools
<b>Other Information Content</b>	<b>Hardware</b>
Databases and data files Back-up and archive data Audit data Paper records and reports Commercial / procurement / supplier information Corporate information e.g. procurement strategy, financial plans etc. Bulk information (any information that is stored in bulk)	Computing hardware including PCs, Laptops, communications devices e.g. smartphones and removable media
<b>System/Process Documentation</b>	<b>Miscellaneous</b>
Intellectual Property e.g. project information Communications information (internal and external) System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Business continuity plans	Environmental services e.g. power and air-conditioning People skills and experience Shared service including Networks and Printers Computer rooms and equipment



---

## Appendix C: Information Asset Owner responsibilities

The IAO and IAA is responsible for working with others, such as Information Governance, Information, IT, corporate and operational leads, to ensure that we are meeting national requirements as set out in the Data Security and Protection Toolkit (DSPT); and our obligations under the data protection legislation. This includes adhering to Trust policies, developing and implementing processes and procedures and contributing to evidence to demonstrate compliance as part of the annual assessment for the Trust. The key areas of focus include: data quality, records management, know your asset, IT protection, and liaising with suppliers.

Responsibilities include:

- assisting the Information Risk Manager in their duties through providing all appropriate information and support
- ensuring that their staff are aware of their data protection responsibilities
- consulting the Information Risk Manager on new developments or issues
- affecting the use of personal data in the organisation
- ensuring Data Protection Impact Assessments (DPIAs) are conducted as appropriate on data processing activities in their business area, drawing on advice from the Data Protection Officer. IAOs must ensure that information risk assessments are performed on all information assets where they have been delegated 'ownership', following guidance from the SIRO and following the Trust risk strategies, policies, code of practice and procedures
- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset
- know who has access to the asset (whether system, portable technology, or information) and why, and ensure access is monitored and compliant with Policy
- understand and address risks to the asset
- foster a culture that values, protects and uses information for the benefit of patients, Employees and the Trust as a whole
- provide assurance to the SIRO on the security and use of information assets
- advise the SIRO regarding Business-Critical Information Assets in keeping with the Information Risk Management Policy and Business Continuity and Disaster Recovery – Information Security Policy
- to comply with the Data Security and Protection Toolkit (DSPT) Standards 1-10 with regards to the information asset, including responding to requests for documented evidence as part of the annual assessment

There are 10 National Data Guardian standards as set out below:

- Standard 1 – Personal confidential data
- Standard 2 – Staff responsibilities
- Standard 3 – Training
- Standard 4 – Managing access
- Standard 5 – Process review
- Standard 6 – Responding to incidents

Standard 7 – Continuity planning  
Standard 8 – Unsupported systems  
Standard 9 – IT Protection  
Standard 10 – Accountable suppliers

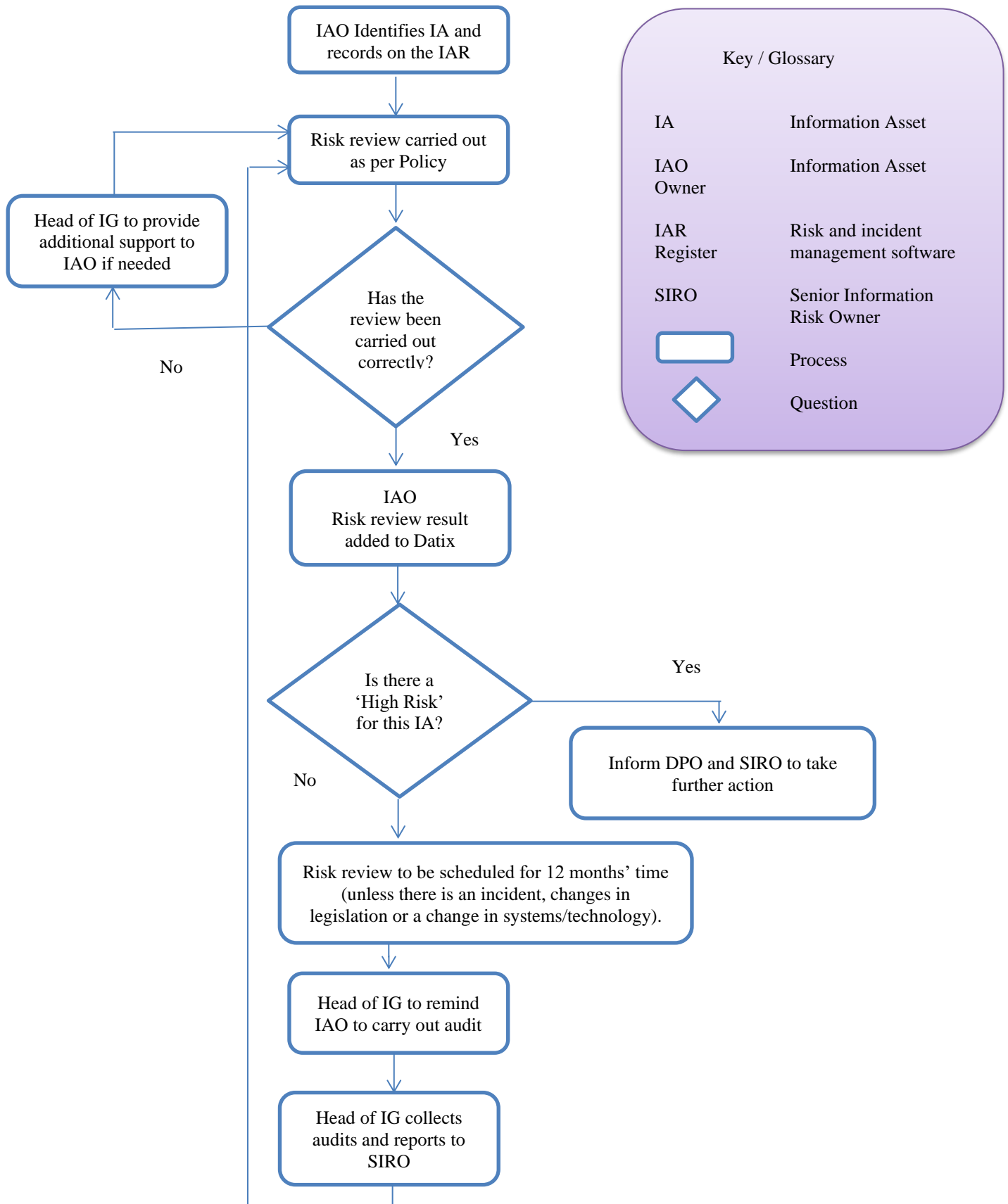
Full guidance can be found here [Help \(dsptoolkit.nhs.uk\)](https://dsptoolkit.nhs.uk)

The above guidance documents will form the foundation for discussion, learning and actions at the IAO and IAA Network groups to ensure that we are pro-actively working towards, contributing to and improving compliance.



Policies that are specifically related to the IAO and IAA roles are:

- Information Risk Policy
- Data Protection Policy (including confidentiality)
- Individual Rights Policy
- Information Security Policy
- Information Quality Assurance
- National Data Opt-Out
- Incident Reporting Policy
- Incident Reporting on Datix

## Appendix D: Risk Review Procedure for Information Assets



**Key / Glossary**

IA	Information Asset
IAO Owner	Information Asset
IAR Register	Risk and incident management software
SIRO	Senior Information Risk Owner
	Process
	Question