Yeovil District Hospital NHS
NHS Foundation Trust

Information Governance Policy

Version Number	5	Version Date	October 2018
Policy Owner	Chief Information Officer		
Author	Data Protection Officer		
First approval or date last reviewed	January 2015		
Staff/Groups Consulted	Information Governance Steering Group		
Draft agreed by Policy Owner	December 2018		
Discussed by Policy Group	December 2018		
Approved by Information Governance Steering Group	8 January 2019		
Next Review Due	October 2021		
Policy Audited			
Equality Impact Assessment Completed	October 2018		

CONTENTS

INFORMATION GOVERNANCE POLICY

1. RATIONALE

1.1 Information is a vital asset, both for the clinical management of individual patients and the efficient management of services and resources. Information Governance plays a key part in clinical and corporate governance, service planning and performance management.

1.2 The Trust has a legal obligation to protect all information it holds, and it is therefore of paramount importance to ensure that information is efficiently managed, and management accountability provide a robust governance framework. Failure to uphold this obligation could result in the Information Commissioner's Office issuing a fine of up to 4% of annual global turnover or €20 million (£17 million) whichever is the greater under the General Data Protection Regulations 2016 and the Data Protection Act 2018 (Data Protection Legislation).

2. INFORMATION GOVERNANCE PRINCIPLES

2.1 Yeovil District Hospital NHS Foundation Trust (YDH) undertakes to implement Information Governance effectively and will ensure the following:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information governance training will be available to all staff as necessary to their role
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated

2.2 Accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

2.3 There are 4 key interlinked strands to the Information Governance Policy: (Annex A)

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

3. AIM

3.1 The aim of this policy is to describe Information Governance arrangements and the processes in place that enable the Trust to meet its responsibilities in the management of information assets and resources. In particular, the arrangement to:

- Hold information securely and confidentially
- Obtain information fairly and efficiently
- Record information accurately and reliably
- Use information effectively and ethically
- Share information appropriately and lawfully

4. DEFINITIONS

4.1 **Information Governance** – Information Governance is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented within the Trust to manage information, supporting the organisation's immediate and future regulatory, legal, risk and operational requirements.

4.2 **Data Security and Protection Toolkit (DSPT) –** The DSPT is a comprehensive and rigorous set of standards describing how information is to be managed in an NHS setting. The organisation self-assesses compliance against these, uploading the necessary evidence to the DSPT portal provided by NHS Digital. Please refer to Annex B.

4.3 **Breach** – A breach refers to an event or action occurring that is in disregard of laws, rules and contracts.

4.4 **Information Commissioners Office (ICO)** – is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

5 ROLES AND RESPONSIBILITIES

Chief Executive

5.1 The Chief Executive has ultimate responsibility for ensuring that the Trust has suitable arrangements in place for the management of Information Governance.

Board of Directors

5.2 The Board of Directors have ultimate responsibility for ensuring that the Trust meets the requirements of the Information Governance agenda and monitors Trust compliance.

5.3 The Board of Directors is the Data Controller for the purposes of the Data Protection Legislation.

5.4 The Board of Directors is responsible for ensuring that information within the Trust is processed according to statutory requirements and arrangements are in place for the management of Data Protection.

5.5 Responsibility for compliance with the standards set out in the DSPT rests with every officer of the Trust, including Executive Directors, Clinical Directors, Business Managers, Matrons, Heads of Departments, Senior Managers, etc.

Strategic Business Units

5.6 Strategic Business Units are required to have comprehensive and robust Information Governance arrangements in place.

5.7 Strategic Business Units have responsibility for the stewardship and management of the information generated, processed or stored within their departments.

5.8 The Joint Strategic Business Unit Meeting accepts delegated responsibility for the identification and management of information management risk in accordance with the Trust Risk Management Strategy.

Heads of Department/Business Managers/Matrons/Clinical Directors

5.9 Heads of Department, Business Managers, Matrons and Clinical Directors will ensure they have local arrangements in place to:

- Support departmental Information Governance arrangements
- Comply with Trust Policies
- Provide evidence for the DSPT
- Oversee status of all risk to the Trust, including information risks

Senior Information Risk Owner (SIRO)

5.10 The SIRO is accountable to the Board of Directors and has overall responsibility for producing the Information Governance Strategy, reporting any information risk issues, addressing any serious incidents, ensuring that the Information Governance standards set by NHS Digital and the DSPT are met.

5.11 The Senior Information Risk Owner (SIRO) is an executive director who takes overall ownership of the organisation's information risk policy, acts as champion for information risk on the Board and provides written advice to the accounting officer (Chief Executive) on the content of the Trust's Annual Governance Statement in regard to information risk.

5.12 The SIRO must understand the strategic business goals of the organisation and how other business goals may be impacted by information risks, and how those risks may be managed.

5.13 The SIRO implements and leads the IG risk assessment and management processes within the organisation and advises the Board on the effectiveness of information risk management across the organisation.

5.14 The Chief Finance and Commercial Officer is the current SIRO at YDH and is supported in specialist functions by the Information Governance Steering Group.

Caldicott Guardian

5.15 The Caldicott Guardian is responsible for ensuring patient confidentiality, information sharing, data privacy and the use of patient data in research according to the Caldicott Principles and the precepts of this policy. The Caldicott Guardian oversees disclosures of patient information including extraordinary disclosures (those which are not routine) in accordance with the 'NHS Confidentiality Code of Practice' (November 2003).

5.16 The Caldicott Guardian plays a key role in ensuring that NHS organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing IG requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

5.17 The Medical Director is the Trust's current Caldicott Guardian.

Data Protection Officer

5.18 The Trust, as a public authority, appointed a Data Protection Officer for the purposes of the General Data Protection Regulations.

5.19 The Data Protection Officer will:

- Inform and advise the Trust and its employees who carry out processing of their obligations pursuant to the Data Protection Legislation
- Monitor compliance with the Data Protection Legislation and Trust policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits
- Provide advice where requested as regards data protection impact assessments and monitor performance against such assessments
- Co-operate with the ICO
- Act as the contact point for the ICO on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- Report matters of compliance or risk direct to the Trust Board and SIRO where it is considered appropriate to do so in addition to using the Trust's existing risk management processes and provide an annual data protection assurance statement to the Trust Board as part of the Annual Governance Statement
- Be responsible for providing specialist Information Governance advice
- Ensure the DSPT is submitted accurately and on time
- Ensure that the Trust fulfils Individual rights under Data Protection Legislation including Data Subject Access Requests

5.20 The DPO & Information Governance and Medical Records Manager are jointly responsible for reporting any Data Protection breaches to the Information Governance Steering Group and if necessary informing the ICO.

Associate Director – Informatics and Transformation

5.21 The Associate Director – Informatics and Transformation is accountable to the Chief Information Officer. The Associate Director – Informatics and Transformation is responsible for the Information Governance and Medical Records Manager, the Medical Records department, the Information department, monitoring the progress of Information Governance compliance and the completion of the DSPT.

Information Governance and Medical Records Manager

5.22 The Information Governance and Medical Records Manager is accountable to the Associate Director – Informatics and Transformation and is responsible for:

- Providing support and delivering the appropriate education to all individuals to ensure they are clear about their responsibilities when handling information
- Ensuring legal requirements are met
- Meeting the performance assessment requirements of the DSPT
- Managing its obligations, issue and support standards, policies and procedures ensuring information is held, obtained, recorded, used and shared correctly

5.23 The DPO & Information Governance and Medical Records Manager are jointly responsible for reporting any Data Protection breaches to the Information Governance Steering Group and if necessary informing the Information Commissioners Officer.

Registration Authority Lead

5.24 The key task of the Registration Authority Lead is to verify the identity of trust staff who need access to sensitive data, and to establish and provide only the degree of access they need to do their jobs.

5.25 Manage the issuing service of Smartcard to staff.

5.26 Ensure that all RA procedures are carried out in accordance with the national policy.

IT Operations Manager

5.27 The IT Operations Manager is responsible for ensuring technological security of information including, but not exclusively, access control and identity management, virus protection, malware protection, anti-phishing measures, and physical security of electronic systems under the care of Information Management & Technology Department.

Information Governance Steering Group

5.28 Information Governance management across the organisation is co-ordinated by the Information Governance Steering group. The role of this group is to:

- Support and drive the broader Information Governance agenda
- Provide the Board with the assurance that effective Information Governance best practice mechanisms are in place across the organisation
- Regularly review compliance with Information Governance related policies and any management issues that arise from them
- Maintain an Information Governance Risk Register
- Review any breaches of the Data Protection Legislation as logged on the Trust's Incident Reporting System (Ulysses Safeguard)
- Provide formal evidence of compliance across Information Governance disciplines to support the annual Data Security and Protection Toolkit submission
- Raise awareness of any incidents to the SIRO for escalating to the Board of Directors and Chief Executive
- Oversee the implementation of areas of work that sit within the Information Governance Framework. These are:
    - Freedom of Information
    - Information Security
    - Data Protection
    - Confidentiality
    - Records Management
    - Health Records

5.29 Terms of Reference for the group are to be reviewed annually by the Steering Group and are presented to the Audit Committee for approval.

Asset Owners

5.30 Information Asset Owners (IAO) have a key role to play in ensuring compliance with this policy. In particular, they have responsibility for ensuring appropriate security is in place for their assets which hold personal data and that staff are adequately trained to use them. They have specific responsibility for managing the content of, access to, use and transfer of and disposal of the personal data within the information assets and that there is a lawful basis for holding and processing the data.

All Staff

5.31 Users of information must:

- Understand their legal obligation to keep personal information confidential, to ensure they do not breach the data protection principles and uphold individual's rights and that failure to comply may result in disciplinary action
- Participate in induction, mandatory and awareness training sessions

- Be aware of the Trust's nominated Information Governance and Medical Records Manager, Data Protection Officer and Caldicott Guardian
- Challenge and verify where necessary the identity of any person who is making a request for confidential information and determine the validity of the reason for requiring that information
- Report actual or suspected breaches of confidentiality
- Ensure data is recorded accurately and in a legible manner

6 PROCESS

6.1 The Trust will ensure that arrangements are in place for monitoring and improving the management of information within the Trust and between the Trust and other organisations or individuals.

6.2 Trust Governance arrangements will be maintained and strengthened by the annual process of compliance with the DSPT.

6.3 Information Governance related policies will be maintained and updated as appropriate with any operational improvements implemented.

6.4 Comprehensive and robust Information Governance arrangements will be implemented to ensure compliance with Trust policies and provide evidence for DSPT returns.

7 BREACHES

7.1 The Data Protection Legislation introduces a duty on data controllers and data processors to report certain types of personal data breaches which meet the criteria of the DSPT IG Incident Matrix to the relevant supervisory authority. There is a requirement this must be completed by the data controller within 72 hours of becoming aware of the breach. Data Processors are required under Article 33(2) to inform the data controller without undue delay as soon as they become aware of a breach.

7.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, data controllers must also inform those individuals without undue delay.

7.3 All data controllers and data processors should have robust breach detection, investigation and internal reporting procedures in place to facilitate decision-making about whether or not the incident needs to be notified to the relevant supervisory authority and the affected individuals.

7.4 All staff have a duty to report any breaches to their Manager, Data Protection Officer and Information Governance Manager under the Trust's Incident Reporting and Investigation Management Policy and Trust Risk Management Strategy. This will be reported through the Trust Incident Reporting System and if a theme or risk is identified, recorded on the Risk Register.

7.5 Where a breach has occurred, disciplinary action may be taken and working practices and procedure will be reviewed.

7.6 Serious breaches, or serious untoward incidents, will be addressed by the Trust Data Protection Officer and Information Governance Manager, by raising a Serious Untoward Incident Form on the DSPT and by informing the ICO.

7.7 Under the Data Protection Legislation data controllers and data processors are required to keep a record of any personal data breaches, regardless of whether the breach has reached the threshold to notify the relevant supervisory authority. This information is held on the individual incident report within the Trust's Incident Reporting System.

7.8 Failing to notify a breach when required to do so can result in a significant fine for the data controller and/or data processor by the ICO. The fine can be combined with the ICO's other corrective powers under Article 58 GDPR.

8 YEAR ON YEAR IMPROVEMENT PLAN AND ASSESSMENT

8.1 Assurance regarding the management of Information Governance arrangements form part of the DSPT.

8.2 An assessment of compliance with requirements will be undertaken each year.

8.3 Annual reports and proposed action/development plans will be presented to the IGSG for approval of submission to the DSPT.

9 TRAINING

9.1 Information Governance forms part of the Staff Trust Induction and Mandatory Training Programme. All staff are required to undertake training annually.

9.2 Staff with additional Information Governance responsibilities will be identified at local induction and annual appraisal. The appropriate training will then be provided.

9.3 All training provided will be recorded on the individuals Electronic Staff Record (ESR) and centrally by the Academy Team.

9.4 Agency, contract staff and employees of subsidiary companies of YDH are subject to the same rules as substantive members of YDH staff.

10 APPLICABILITY

10.1 This policy applies to staff employed by the Trust, including contract and temporary staff. Patients, visitors and the general public will be made aware of this Policy as required. Failure to comply with this policy may lead to disciplinary action in line with the Discipline Policy contained within the HR Manual.

10.2 Any employees of subsidiary companies of YDH will adhere to this policy and will receive consistent training in relation to policy implementation.

11 IMPLEMENTATION, MONITORING AND EVALUATION

11.1 Data Protection compliance will be monitored through:

- The Information Governance Steering Group
- DSPT annual submission (baseline assessment October each year and final submission in March each year)
- Incident Reports
- Audits
- External Reports
- The number of reportable information governance and data protection incidents
- Compliance with time limits for individual rights

12 REFERENCES AND ASSOCIATED DOCUMENTS

- General Data Protection Regulations 2016
- Data Protection Act 2018
- Information Governance Policy
- Data Protection Policy

- Freedom of Information Act 2000 Policy
- Staff Code of Confidentiality
- Corporate Records Management Policy
- Information Security Policy
- Data Quality Policy
- Health Record Keeping and Management Policy
- Caldicott Guardian Approval Procedure
- Incident Reporting and Investigation Management Policy
- Risk Management Strategy and Policy
- Human Resources Manual – which includes Staff Conduct and Disciplinary Policies
- Standard Operating Procedure for the Management of Individual Rights under the Data Protection Legislation
- 2017/18 Data Security and Protection Requirements
- NHS Confidentiality Code of Practice' (November 2003)
- NHS Digital Data Security and Information Governance Guidance
- Information Commissioner's Office web site: http://www.ico.gov.uk
- DSPT: https://www.dsptoolkit.nhs.uk

ANNEX A – KEY PRINCIPLES OF INFORMATION GOVERNANCE

Openness

The Trust recognises the need for an appropriate and proportionate balance between openness and confidentiality in the management and use of information. 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.

Information on the Trust and its services will be made available to the public through a variety of media. These include the Internet website, Annual Reports and Press Releases. Support will be provided for people with special/different needs. Exceptions will only be made where this is necessary to protect the confidentiality of personal or commercially sensitive information or for compliance with other legal obligations.

The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act, Environmental Information Regulations, and Re-Use of Public Sector Information Regulations. It will maintain a Publication Scheme, and guide to available information, on the public website. The Trust will comply with relevant Codes of Practice including those issued under s45 of the Freedom of Information Act and Regulation 16 of the Environmental Information Regulations.

Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients. The Trust adopts and affirms the NHS Care Records Guarantee and in providing people with access to their own information will comply with the Information Commissioner's Privacy Notices and Subject Access Codes of Practice.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

The public, including patients, will be told how information about them is used, and about safeguards governing use of personal data. The Trust will ensure that consent issues will be given thorough consideration before the start of any research or management study, and consent will be obtained, whenever necessary in accordance with a published Consent Policy
Staff will be kept regularly informed of activities within the organisation through briefings and bulletins by email and accessible on the Trust intranet.

Legal Compliance

The Trust will establish and maintain a Data Protection Policy and comply with all legal requirements in the management and handling of information, including personal data, in particular:

- The Access to Health Records Act 1990
- The Care Quality Commission (Registration) Regulations 2009
- The Copyright Designs & Patents Act 1988
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- The General Data Protection regulation 2016 and Data Protection Act 2018
- The Environmental Information Regulations 2004

- The Freedom of Information Act 2000
- The Re-Use of Public Sector Information Regulations 2015
- The Health and Social Care Act 2012
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- The Human Rights Act 1998
- The Law of Confidentiality
- The Public Records Act 1958

In meeting the legal requirements the Trust will have regard to best practice guidance issued by NHS England and others, in particular:

- The Trust will adopt and conform to the guidance issued by the Care Quality Commission on meeting its responsibilities under the appropriate regulations with particular reference to Regulation 17 ("Good Governance") of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- The Trust has appointed a Caldicott Guardian and will at all times adhere to the Caldicott Principles in consultation with the Guardian
- The Trust will use Accredited Safe Havens where appropriate and will conform to the principles, requirements and guidance for Accredited Safe Havens issued by NHS Digital

Annual assessments and audits of the Trust compliance with legal requirements will be undertaken.

Information Security

The Trust will maintain an Information Security Policy for the effective and secure management of information assets and resources. It will include arrangements for controlled access to systems and training, in advance of the granting of access rights.
Transfers of information (whether person identifiable, sensitive, confidential or corporate) into, out of and within the Trust including ad hoc and regular data disclosures and data sharing will be subject to appropriate controls.

The Trust has established and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches (near misses) of confidentiality, loss of personal data, and actual or potential breaches of data security, data integrity and data availability.

The Trust adopts and follows NHS Digital Guidance for reporting, managing and investigating information governance and cyber security serious incidents requiring investigation (SIRI's). Please refer to the Trust's Incident Reporting and Investigation Management Policy for further information.
The Trust will ensure that all contracts with data processors contain appropriate safeguards in accordance with the seventh data protection principle and that due diligence is exercised in the appointment of such contractors.

The Trust will comply with the NHS Information Security Management Code of Practice and will seek to adopt standards which conform to the BS ISO/IEC 27000 series - the international Standards that describes best practice for an information security management systems and controls.

The Trust will adopt and use the UK Security Classification Framework where appropriate for the protective marking of information, and in particular when sharing health and social care information.

The Trust will adopt and apply NHS Digital guidance on:

- Standards for cryptographic algorithms and key sizes
- Disposal and destruction of sensitive data
- General principles for securing information systems
- Implementing business continuity planning and disaster planning procedures

Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records. Information Asset Owners are expected to seek to continuously improve the quality of information within their services. Wherever possible, information quality should be assured at the point of collection.

The Trust will ensure that appropriate audits are carried out to monitor compliance with this policy.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards. The Trust will have regard to guidance on data quality issued by NHS Digital and maintains a Data Quality Policy.

The Trust will, subject to the proviso below, adopt and seek to apply national standards of best practice in the management and handling of information, whether from NHS England or otherwise, including:

- Information Commissioner's Anonymisation Code of Practice
- Information Commissioner's Privacy Impact Assessments Code of Practice
- Records Management Code of Practice for Health and Social Care 2016 or any revision thereof. The Trust will, subject to the proviso at 3.21, follow the retention schedule set out in Section 4 of the Code
- Code of Practice on Records Management under s46 Freedom of Information Act 2000
- The Statutory Code of Practice on confidentiality issued by NHS Digital in 2014 under s263 of the Health and Social Care Act 2012 and the DoH 2003 NHS Confidentiality Code of Practice, together with the NHS Digital Guide to Confidentiality in Health & Social Care issued in 2013 (including the References Document). Trust staff are required at all times to comply with the five confidentiality rules set out in the 2013 Guide. Where public interest disclosures are concerned the Trust adopts the DoH Supplementary Guidance issued in 2010

In managing the confidentiality of personal confidential data the Trust will also apply the Caldicott principles.

Where for good and sufficient reason the Trust departs from any such guidance the decision and reasons for adopting an alternative approach will be recorded, in appropriate committee minutes and / or any applicable policy or guidance issued by the Trust.

The Trust encourages the sharing of information within the Trust and between the Trust and other NHS and partner organisations, including health and social care professionals, to support patient care as determined by law, statute and best practice provided there is a legitimate basis for doing so, and in accordance with the Caldicott principles and the Information Commissioner's Data Sharing Code of Practice.

All staff will be required to undergo annual training in Information Governance. Further training as appropriate will be required for staff with specialist Information Governance roles

ANNEX B – NHS DIGITAL
DATA SECURITY AND PROTECTION TOOLKIT (DSPT) REQUIREMENTS

Background

From April 2018 the new Data Security and Protection Toolkit (DSPT) replaces the Information Governance Toolkit (IG Toolkit). It forms part of the new framework for assuring that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security.

The ten data security standards apply to all health and care organisations. When considering data security as part of the well-led element of their inspections, the Care Quality Commission (CQC) will look at how organisations are assuring themselves that the steps set out in this document are being taken. More information on the CQC inspection frameworks can be found here: http://www.cqc.org.uk/guidance-providers

NHS Providers

Organisations contracted to provide services under the NHS Standard Contract (NHS providers) must comply with the requirements set out in the DSPT, as part of the data security and protection requirements set out in that contract. At the end of the 2017/18 financial year NHS Improvement asked NHS providers to confirm they have implemented the requirements set out in this document. In the longer term NHS Improvement will ensure data security is included in NHS Provider's oversight arrangements.

Completing the DSPT self-assessment, by providing evidence and judging whether as an organisation we have met the assertions, will demonstrate that the Trust is working towards or meeting the NDG standards:

1 Personal Confidential Data
2 Staff Responsibilities
3 Training
4 Managing Data Access
5 Process Reviews
6 Responding to Incidents
7 Continuity Planning
8 Unsupported Systems
9 IT Protection
10 Accountable Suppliers

1 Personal Confidential Data			
All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.			
No.	**Requirement**	**Owner**	**Mandatory**
1.1	**There is senior ownership of data security and protection within the organisation.**	Information Governance and Medical Records Manager	Yes
1.1.1	Name of Senior Information Risk Owner		Yes
1.1.2	SIRO Responsibility for data security has been assigned		Yes
1.1.3	Name of Caldicott Guardian		Yes
1.1.4	Who are your staff with responsibility for data protection and/or security?		Yes
1.1.5	Staff awareness - Leadership (Q1) I feel data security and protection are important for my organisation		No
1.1.6	Name of Appointed Data Protection Officer		Yes
1.2	**There are clear data security and protection policies in place and these are understood by staff and available to the public.**		Yes
1.2.1	There is a data security and protection policy or policies that follow relevant guidance.		Yes
1.2.2	When were the data security and protection policy or policies last updated?		Yes

1.2.3	Data Security and Protection Policy has been approved by the SIRO	Information Governance and Medical Records Manager	Yes
1.2.4	Data Security and Protection Policies available to the public.		No
1.2.5	Staff awareness - Policies (Q2). I know the rules about who I share data with and how.		No
1.2.6	Staff awareness – Policies (Q3). I know who to ask questions about data security in my organisation.		No
1.3	**Individuals' rights are respected and supported (GDPR Art 12-22)**		Yes
1.3.1	ICO Registration Number.		Yes
1.3.2	Transparency information is published and available to the public.		Yes
1.3.3.	How have Individuals been informed about their rights and how to exercise them?		Yes
1.3.4	There is a staff procedure about how to provide information about processing and individuals' rights at the correct time.		Yes
1.3.5	There is an updated subject access process to meet shorter GDPR timescales.		Yes
1.3.6	Provide details of how access to information requests have been complied with during the last twelve months.		Yes
1.3.7	Have there been any ICO actions taken against the organisation in the last 12 months, such as fines, enforcement notices or decision notices?		No
1.4	**Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)**		
1.4.1	A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied.		Yes
1.4.2	Have information flows been approved by the SIRO or equivalent local method?		
1.4.3	Date of when information flows were approved by the Board or equivalent.		
1.4.4	Provide a list of all systems/information assets holding or sharing personal information.		
1.4.5	List of systems which do not support individual login with the risks outlined and what compensating measures are in place.		
1.5	**Personal information is used and shared lawfully.**		Yes
1.5.1	There is approved staff guidance on confidentiality and data protection issues.		Yes
1.5.2	Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed.		Yes
1.5.3	Results of staff spot checks and actions taken when data protection non-compliance is identified.		Yes
1.5.4	Staff awareness - Used legally and securely (Q4) …. I am happy data is used legally and securely in my organisation		No
1.6	**The use of personal information is subject to data protection by design and by default**		Yes
1.6.1	There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.		Yes
1.6.2	Data Protection by design procedure agreed by local governance process.		Yes
1.6.3	There are technical controls that prevent information from being inappropriately copied or downloaded.		Yes
1.6.4	There are physical controls that prevent unauthorised access to sites.		Yes
1.6.5	Date of last audit of pseudonymisation, anonymisation or de-identification controls.		Yes
1.6.6	Overall findings of last audit of [pseudonymisation, anonymisation or de-identification] controls.		Yes
1.6.7	There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.		Yes
1.6.8	The Data Protection Impact Assessment Procedure has been agreed by the Board or equivalent.		Yes
1.6.9	The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessment is being carried out.		No
1.6.10	Have any unmitigated risks been identified through the Data Protection Impact Assessment process?		Yes
1.6.11	All high risk data processing has a Data Protection Impact Assessment carried out before processing commences.		Yes
1.6.12	All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.		Yes
1.6.13	Data Protection Impact Assessments are published and available as part of		Yes

	the organisation's transparency materials.		
1.7	**Effective data quality controls are in place**	Performance and Reporting Manager	Yes
1.7.1	There is policy and staff guidance on data quality.		Yes
1.7.2	The scope of the data quality audit was in line with guidelines.		Yes
1.7.3	Date of last data quality audit.		Yes
1.7.4	Overall findings of last audit of data quality.		No
1.8	**Personal information processed by the organisation is adequate (and not excessive) for the purposes.**	Information Governance and Medical Records Manager	Yes
1.8.1	There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.		Yes
1.8.2	A records retention schedule has been produced.		Yes
1.8.3	Provide details of when personal data disposal contracts were last reviewed/updated.		Yes
1.8.4	Date of last audit being made on data disposal contractors to ensure security is of the appropriate agreed standard.		Yes
1.8.5	Number of destruction certificates received from data disposal contractors in the last 12 months.		No

2 Staff Responsibilities			
All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.			
No.	**Requirement**	**Owner**	**Mandatory**
2.1	**There is a clear understanding of what Personal Confidential Information is held.**	IT Operations Manager	Yes
2.1.1	When was the last review of the list of all systems/information assets holding or sharing personal information?		
2.1.2	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the SIRO or equivalent local method.		
2.2	**Personal Confidential Information is processed/shared legally and securely.**	Information Governance and Medical Records Manager	No
2.2.1	Staff awareness - Shared securely (Q5) …. I know how to use and transmit data securely.		
2.2.2	Staff awareness - Used legally and securely (Q6) …. I feel that confidentiality is more important than sharing information for care.		
2.2.3	Staff awareness - Processes (Q7) …. The tools and processes used by my organisation make it easy to use and transmit data securely.		
2.2.4	Staff awareness - Raising concern (Q8) …. I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination.		
2.3	**Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.**	Information Governance and Medical Records Manager	Yes
2.3.1	There is a data protection and security induction in place for all new entrants to the organisation.		Yes
2.3.2	All employment contracts contain data security requirements.		Yes
2.3.3	Staff awareness - Laws and principles (Q9) …. I understand the important laws and principles on data sharing, and when I should and should not share data.		No
2.3.4	Staff awareness - Data sharing questions (Q10) …. If I have a question about sharing data lawfully and securely I know where to seek help.		No
2.3.5	Staff awareness - Personal responsibility (Q11)…. I take personal responsibility for handling data securely.		No

3 Training			
All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.			
No.	**Requirement**	**Owner**	**Mandatory**
3.1	**There has been an assessment of data security and protection training needs across the organisation.**	Information Governance and Medical Records Manager	Yes
3.1.1	A data security and protection training needs analysis has been completed.		
3.1.2	Date of last data security and protection training needs analysis.		
3.1.3	Training Needs analysis has been approved by the SIRO or equivalent.		
3.2	**Staff receive suitable data security and protection training.**		No
3.2.1	Staff awareness - Training (Q12) … The data security training offered by my organisation supports me in understanding how to use data lawfully and securely.		
3.3	**Staff pass the data security and protection mandatory test.**		Yes
3.3.1	Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.		Yes
3.3.2	Average mark of first attempt of Level 1 Training.		No
3.4	**Staff with specialist roles receive data security and protection training suitable to their role.**		Yes
3.4.1	Number of staff assessed as needing role specialist training.		
3.4.2	Number of staff completing specialist Data Security Training.		
3.4.3	Details of any specialist data security and protection training undertaken.		
3.5	**Leaders and board members receive suitable data protection and security training.**		Yes
3.5.1	SIRO and Caldicott Guardian have received appropriate data security and protection training.		
3.5.2	List of Board Members.		
3.5.3	Percentage of Board Members completing appropriate data security and protection Training.		

4 Managing Data Access			
Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.			
No.	**Requirement**	**Owner**	**Mandatory**
4.1	**The organisation maintains a current record of staff and their roles.**	IT Operations Manager	Yes
4.1.1	Confirmation that the organisation maintains a current record of staff and their roles.		
4.1.2	For each system holding personal and confidential data, the organisation understands who has access to the information.		
4.2	**Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.**		Yes
4.2.1	Date last audit of user accounts held.		Yes
4.2.2	List of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.		No
4.2.3	Staff awareness - Access to information (Q13): The level of access I have to IT systems holding sensitive information, is appropriate.		No
4.3	**All staff understand that their activities on IT systems will be monitored and recorded for security purposes.**		Yes
4.3.1	All system administrators have signed an agreement which holds them accountable to the highest standards of use.		Yes
4.3.2	The Head of IT, or equivalent, confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.		No
4.3.3	Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder.		No
4.3.4	List of all systems to which users and administrators have an account, plus the means of monitoring access		Yes
4.3.5	Staff have provided explicit understanding that their activity of systems can be monitored.		Yes

5 Process Reviews			
Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.			
No.	**Requirement**	**Owner**	**Mandatory**
5.1	**Process reviews are held at least once per year.**	IT Operations Manager	Yes
5.1.1	Dates of process reviews held to identify and manage problem processes which cause security breaches.		Yes
5.1.2	List of actions arising from the process review, with names of actionees.		No
5.2	**Participation in reviews is comprehensive, and clinicians are actively involved.**		No
5.2.1	Scanned copy of the process review meeting registration sheet with attendee signatures and roles held.		
5.3	**Action is taken to address problem processes as a result of feedback at meetings or in year.**		No
5.3.1	Explain how the actions to address problem processes are being monitored and assurance given to the Board or equivalent senior team?		

6 Responding to Incidents			
Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.			
No.	**Requirement**	**Owner**	**Mandatory**
6.1	**A confidential system for reporting security breaches and near misses is in place and actively used.**	Data Protection Officer	Yes
6.1.1	A data security and protection breach reporting system is in place.		Yes
6.1.2	List routes available for staff to report data security and protection breaches and near misses.		No
6.1.3	List of all data security breach reports in the last twelve months with action plans.		Yes
6.1.4	The Board or equivalent is notified of the action plan for all data security breaches.		Yes
6.1.5	Individuals affected by a breach are appropriately informed.		Yes
6.2	**Users know how to spot an incident and where to report it, and incidents are effectively reported.**	Data Protection Officer	Yes
6.2.1	Number of data security and personal information breaches recorded.		No
6.2.2	Speed of data security and protection breach reporting.		No
6.2.3	Staff awareness - Reporting (Q14) - I know how to report a data security breach.		No
6.2.4	Number of breaches that have been reported to the Information Commissioner.		Yes
6.3	**All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.**	IT Operations Manager	Yes
6.3.1	Name of anti-virus product.		
6.3.2	Number of alerts recorded by the AV tool in the last three months.		
6.3.3	Name of spam email filtering product.		
6.3.4	Number of spam emails blocked per month.		
6.3.5	Number of phishing emails reported by staff per month.		
6.4	**Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.**	Data Protection Officer	Yes
6.4.1	Number and details of incidents caused by a known vulnerability being exploited.		Yes
6.4.2	Have you had any repeat data security incidents of the same issue within the organisation.		No
6.4.3	Staff awareness - Incidents (Q 15) - When there is a data security incident my organisation works quickly to address it.		No
6.4.4	Staff awareness - Learning Lessons (Q16) - When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again.		No

7 Continuity Planning			
A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.			
No.	**Requirement**	**Owner**	**Mandatory**
7.1	**There is a continuity plan in place for data security incidents, and staff understand how to put this into action.**	IT Operations Manager	Yes
7.1.1	There is an incident management and business continuity plan in place for data security and protection.		Yes
7.1.2	The incident management and business continuity plan has been approved by the SIRO or equivalent senior role.		No
7.1.3	Staff awareness - Contingency plan (Q17) - If a data security incident was to prevent technology from working in my organisation, I know how to continue doing the critical parts of my job.		No
7.1.4	Document any updated processes to improve responses to common forms of incidents.		No
7.2	**There is an effective annual test of the continuity plan for data security incidents.**		Yes
7.2.1	Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.		Yes
7.2.2	Which scenario was rehearsed during the business continuity exercise, why, and when?		No
7.2.3	From the business continuity exercise which issues and actions were documented, with names of actionees listed against each item.		No
7.2.4	All emergency contacts are kept securely, in hardcopy and are up-to-date.		Yes
7.2.5	Location of hardcopy of emergency contacts.		Yes
7.2.6	Date emergency contact list updated.		Yes
7.2.7	Date emergency contact list printed/shared.		No
7.2.8	Draft Press materials for data security incidents.		No
7.2.9	Date press materials for data security incidents last updated.		No
7.2.10	Document any re-defined processes to respond to common forms of cyber-attack in the last twelve months.		Yes

8 Unsupported Systems			
No unsupported operating systems, software or internet browsers are used within the IT estate.			
No.	**Requirement**	**Owner**	**Mandatory**
8.1	**All software has been surveyed to understand if it is supported and up to date.**	IT Operations Manager	Yes
8.1.1	What software do you use?		
8.2	**Unsupported software is categorised and documented, and data security risks are identified and managed.**		Yes
8.2.1	List of unsupported software prioritised according to business risk, with remediation plan against each item.		
8.2.2	Where it is not possible to upgrade/update software, reasons are given.		
8.2.3	The SIRO confirms that the risks of using unsupported systems are being treated or tolerated.		
8.3	**Supported systems are kept up-to-date with the latest security patches.**		Yes
8.3.1	Provide your strategy for security updates.		
8.3.2	How regularly do you apply security updates to desktop infrastructure.		
8.3.3	How often, in days, is automatic patching typically being pushed out to remote endpoints?		
8.3.4	How many times, in the last twelve months has the SIRO or equivalent senior role been notified where patches have not been applied for longer than two months, with reasons why?		
8.3.5	List of where software updates have not been applied for longer than two months, with reasons why.		

9 IT Protection			
A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.			
No.	**Requirement**	**Owner**	**Mandatory**
9.1	**All networking components have had their default passwords changed.**	IT Operations Manager	Yes
9.1.1	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed.		
9.1.2	A Penetration test has been conducted in the last 12 months, which confirmed that all networking components have had their default passwords changed.		
9.2	**Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities.**		No
9.2.1	A penetration test has been conducted in the last 12 months, which confirmed web applications were not vulnerable to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities.		
9.2.2	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with action plan against outstanding OWASP findings.		
9.3	**All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them.**		Yes
9.3.1	The annual IT penetration testing is scoped in negotiation between the business and the testing team, and uploaded.		
9.3.2	The SIRO confirms the scope of the annual IT penetration testing is adequate, and that actions from the previous penetration testing are complete or ongoing (with reasons for non-completion).		
9.3.3	The date the penetration test was undertaken.		
9.4	**A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.**		Yes
9.4.1	The SIRO or equivalent senior role confirms the organisation has a data security improvement plan.		Yes
9.4.2	What are your top three data security and protection risks?		Yes
9.4.3	Evidence that your board has discussed your top three data security and protection risks and what is being done about them?		Yes
9.4.4	Date for full implementation of the data security improvement plan.		No
9.4.5	Data security improvement plan status.		Yes

10 Accountable Suppliers			
IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.			
No.	**Requirement**	**Owner**	**Mandatory**
10.1	**The organisation can name its suppliers, the products and services they deliver and the contract durations.**	IT Operations Manager	Yes
10.1.1	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.		Yes
10.1.2	Contracts with all third parties that handle personal information are compliant with GDPR.		No
10.2	**Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance.**		Yes
10.2.1	Basic due diligence has been undertaken against each supplier according to ICO guidance.		Yes
10.2.2	Percentage of suppliers with data security contract clauses in place.		Yes
10.2.3	Statements have been received from all Suppliers that handle personal information on their preparedness for GDPR.		No
10.2.4	Board, or equivalent, assured that suppliers who are Data Processors are prepared for GDPR.		No
10.3	**All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.**		No
10.3.1	List of data security incidents – past or present – with current suppliers.		

10.4	**All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at board**		No
10.4.1	List of instances of not complying with National Data Guardian standards by suppliers, with date discussed at board or equivalent level.		
10.5	**Where a supplier processes or has access to personal confidential information they have completed a Data Security and Protection Toolkit.**		No
10.5.1	All Suppliers that process or have access to personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.		No

ANNEX B – 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 / N/A	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 including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability	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?	N/A	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	N/A	
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 the Trust's lead for Equality & Diversity, together with any suggestions as to the action required to avoid / reduce this impact.

For advice in respect of answering the above questions, please contact the Trust's lead for Equality & Diversity.

Signed – Samantha Hann, Data Protection Officer **Date –** October 2018