Policy Document

Reference: DSP18 (DSP07)

University Hospitals of North Midlands NHS Trust

Over-arching Data Security & Protection Policy

Version:	**10**
Date Ratified:	**February 2021 by Executive Data Security & Protection Group**
Date of Issue:	**April 2021**
To Be Reviewed Before:	**February 2024**
Policy Author:	**Data Security & Protection Manager**
Executive Lead:	**Senior Information Risk Owner**

Version Control Schedule

Version	Issue Date	Comments
1	January 2005	Policy developed and approved.
2	April 2009	
3	January 2013	Approved by IGSG as part of Information Governance process, List of Policies on p6 corrected, approved using Chairs Action Updated and 4.1 for Compliance reasons, and References. Approved by IGSG.
4	December 2013	Ratified by Quality and Safety Forum. Minor changes: Pg. 7 – removed SHA and CfH. Added in HSCIC. Pg. 8 and 9 – added SIRO and Caldicott Guardian IG training to be competed annually. Pg. 11 – role of clinical audit and support manager added. Pg. 11 – incident reporting added.
5	October 2014	Page 11 – changed clinical audit and compliance support manager job title to information governance facilitator. Page 11 – added contact email address for IG department.
6	January 2015	Policy re-developed in line with IG toolkit requirement 101 which outlines what needs to be in the Framework, and to provide one policy across the Royal Stoke and County Hospital sites.
7	December 2018	Updated to reflect latest legislation, including GDPR and the Data Protection Act. Updated to reflect updates to the Data Security & Protection Toolkit
8	January 2020	Updated for Data Security & Protection Toolkit. Training Needs Analysis (Appendix 1) added. Definitions (Appendix 2) added. Monitoring Table added (Pg. 8) added.
9	February 2020	Page 5 – updated to include a reference to the National Data Opt Out Scheme
10	February 2021	Re-draft/New Policy

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

CONTENTS **Page**

1. INTRODUCTION

This overarching Data Security & Protection Policy defines the Trust's operational approach to meeting the Data Security & Protection Strategy which details the requirements for compliance and effective management in each of the following areas of data security and protection (DSP):

- Confidentiality & Data Protection Act Assurance
- Data Security & Protection Assurance
- Information Security Assurance
- Secondary Use and Information Sharing Assurance
- Communications Assurance

Any Standard Operating Procedures associated with the policies referenced in this document will be regarded as mandatory for staff to adhere to.

An "Equality Impact Assessment" has been completed and no actual or potential discriminatory impact has been identified relating to this document.

2. SCOPE

The Data Security & Protection Policy constitutes the top level of the Trust's Data Security & Protection Assurance Framework (DSPAF). The DSPAF encompasses all relevant policies, processes, standard operating procedures and guidance that meet the five elements of data security and protection, alongside information security within the Trust (listed above)

This is a Trust-wide Policy and applies to all information held regardless of the medium, including but not limitied to electronic, paper, medical devices, CCTV, audio and visual. The policy also applies to information technology (IT) systems and the data held, processed or transmitted by them, all staff, service user, management, audit and all other types of information used by the Trust.

It also covers paper records and manual processes. This is a Trust-wide Policy and applies to all staff and personnel operating under the auspices of the Trust, including employees, locums, contractors, temporary staff, students, service user representatives, volunteers and partner agency staff.

Where a third party has an organisational policy that differs from this policy, a formal agreement as to which policy statement applies shall be outlined and agreed within the contractual documentation. In the absence of such an agreement, this policy shall be deemed to have precedence.

3. DATA SECURITY & PROTECTION GOVERNANCE FRAMEWORK (DSPGF)

The Trust's DSPGF is shown in detail at Appendix 2. All documents are available via the Trust Intranet.

4. LEGAL & COMPLIANCE STANDARDS

The Trust is required to ensure that relevant UK legislation and NHS standards are understood and complied with. The key legislation and standards is not an exhaustive list. The Trust has appropriate policies and processes to meet its legislative and statutory requirements and these are detailed in the DSPGF.

4.1 Key Legislation

- Data Protection Act 2018 and the General Data Protection Regulation (2018)
- The Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Privacy in Electronic Communications Regulations 2003
- Human Rights Act 2000
- Access to Health Records Act 1990

4.2 Key Guidance

- NHS Code of Practice for Records Management
- National Data Opt Out
- NHS Confidentiality Code of Conduct

4.3 Key Standards

- NHS Data Security and Protection Toolkit
- Cyber Essentials Plus
- ISO 27001
- Information Governance Alliance (NHS Digital)
- NHS code of practice(s)

5. ROLES AND RESPONSIBILITIES

The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Performance & Finance Committee will be updated on DSP issues via highlight report, 6 times annually.

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for IG throughout the Trust and is required to provide assurance that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner (SIRO)
The Trust SIRO is responsible to the Chief Executive for Data Security & Protection and acts as an advocate for information risk on the Trust Board.

Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

Head of Data Security & Protection/Data Protection Officer
The Head of Data Security & Protection/Data Protection Officer (DPO) has overall responsibility for managing the data security & protection function and as DPO will advise and monitor compliance with the GDPR and DPA. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the data security & protection agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office.

Head of Data Quality & Clinical Coding
Will work closely with the Data Security & Protection team to provide information quality assurances across all areas of Trust activity. Within this context, the Data Quality Group provides and receives regular reports to and from the Data Security & Protection Executive Group.

Information Asset Owners (IAO)
Designated Information Asset Owners (IAOs) are responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrators (IAA)
Information Asset Owners can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities. IAA ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Where an IAA is not in place, this function is carried out wholly by the IAO.

Data Security & Protection Manager
The Trust's Data Security & Protection Manager is responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda.

Data Security & Protection Facilitator
The Trust's Data Security & Protection Facilitator(s) is responsible for supporting the Data Security & Protection Manager in the delivery of the DSP agenda.

Data Security & Protection Executive Group (DSPEG)
The SIRO and Caldicott Guardian are joint chair of the Trust's DSPEG. This group is responsible for receiving assurances relating to the day to day management of the individual components of the Trust's Data Security & Protection Framework.

Data Security & Protection Operational Group (DSPOG)
The Data Protection Officer chairs the Trust's DSPOG. This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework.

The Data Security & Protection Governance pack provides more detail on the make-up of the Groups which provide assurance that the Trust meets its obligations around data security & protection.

Information Security Manager (RA and Privacy)
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

Cyber Security Lead
Provides advice to theTrust, ensuring compliance and conformance, with local and national requirements and, generally, on cyber security issues across the Trust

Health Records Manager
Oversees the operational management of the Trust's paper health records ensuring that security is maintained in accordance with the legislation. The Health Records function also provides the subject access function for patients to access their clinical records.

Assistant Director of Human Resources/Governance Lead
Has responsibility for ensuring that the HR function meets the legislated requirements of the Data Protection Act 2018 in terms of security of information and access to records by staff (both current and former).

All Staff
All staff, via job roles and contracts of employment/professional registrations must comply with specific data security related legal and ethical obligations and therefore must be aware of the related standards which impact within their area of responsibility. Individual staff must ensure that they make themselves aware of all policies and associated Standard Operation Procedures referenced in this document and abide by their contents. Any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff can email the Data Security & Protection team on DSPUHNM@uhnm.nhs.uk with any data security related queries.

Performance & Finance Committee
The Performance & Finance Committee is the Board Sub-Committee responsible for receiving assurances, on behalf of the Trust Board, that the day to day management of the individual components of the Trust's Data Security & Protection Framework are appropriate and fit for purpose.

6. KEY TASKS

The Data Security & Protection Assurance Framework (DSPAF) covers all compliance and operational requirements. The DSPMS framework and subsidiary supporting policies, processes and guidance is shown in section 2.1 above. Specific key work areas from the DSPMS are outlined below.

6.1 **Data Protection Impact Assessments**
The DSP team is responsible for ensuring data protection impact assessments are carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal and special categories of personal data is handled
.

6.2 **Processing of special category data**
The DSP team will provide specialist advice and guidance on the processing of special category data.

6.3 **Information Flow Mapping**
The DSP team is responsible for ensuring appropriate information flow maps are in place for all IT systems (including but not limited to medical devices; CCTV; Cameras) and operational services (including but not limited to paper records; images)

6.4 **Information Sharing Agreements**
The DSP team is responsible for ensuring appropriate information sharing agreements are in place with our partner organisations.

6.5 **DSP Audits**
The DSP team will conduct regular data security & protection audits. The DSP audits will cover corporate records; confidentiality and information/cyber security. A SOP detailing the process for conducting DSP Audits will be available on the Intranet.

6.6 **Subject Access Requests**
Service user subject access requests will be processed by the Health Records Team.

Staff subject access requests will be processed by the human resources team.

Personal Data Requests (electronic information **not** included within a health record) will be processed by the DSP team (in conjunction with any other teams involved for example, Complaints)

Privacy Information Requests (auditing the Trust systems to identify inappropriate staff access) will be processed by the DSP team, in conjunction with the Trust's H.R. team and in line with the ICO code of practice on Subject Access Requests.

6.7 **Freedom of Information Request**
The DSP team will manage Freedom of Information Requests with assistance from the Trust Divisional teams. All requests will be signed off by the Divisional Executive Leadin line with the Information Commissioner's Code of Practice

6.8 **Corporate Records Management**
The Trust is required to maintain its corporate records to the same standards as clinical records in terms of security, retention, access restrictions etc. The Trust is required to audit departments to ensure that these standards are met and the outcome/results of these audits will be presented to the DSPOG.

6.9 **Information/ Cyber Security**
The DSP team will provide relevant guidance on information security standards and practices including all aspects of cyber security in conjunction with the Cyber Security Lead/IM&T.

6.10 **Advice and Guidance**
The DSP team, will provide subject matter advice where required.

6.11 **Information Asset Management**
The DSP team will maintain the Trusts information asset register and ensure that all new assets meet the requirement for Privacy by Design via the due diligence process

6.12 **Data Security & Protection Incident management**
All DSP incidents will be reported via DATIX in line with the Trust's adverse incident policy and procedures that can be found on the Trust Intranet and reported externally in accordance with the latest requirements for external reporting.

The DSP team will review all incidents reported that have been classified as a DSP incident to ensure that appropriate investigations are undertaken and to identify any incidents that require external reporting within the mandated timeframe.

6.13 **Information Risk Management**
As part of the due diligence process required by the Privacy by Design obligations under the Data Protection Act 2018 and the Trust's Risk Management Policy, the DSP team will undertake a risk assessment of all new systems, procedures and processes. Annual Risk Assessments will also be required as part of the annual review of all assets and the Trust's Information Asset Register.

6.14 **Training**

Mandatory Data Security & Protection training for all staff (whether permanent, temporary or contracted) is included in the Trusts statutory and mandatory training requirements.

All staff will receive training on commencement (Induction) and thereafter the training must be completed via the Trust's on-line e-learning portal on a yearly basis as per the requirements of the Statutory and Mandatory Training Policy (HR53) and Corporate Induction Policy (HR17) as well as the Trust's User Awareness Policy.

Staff that require enhanced/specialised DSP training for their role will be identified on an annual basis and required to also achieve this training requirement. The Trust's Training Needs Analysis can be found at Appendix 1.

The DSP team will produce up dated information in relation to DSP training compliance on a monthly basis and this information will be provided to operational Groups to assist them in meeting their obligations in this area. The Trust compliance against this statutory & mandatory training requirement is monitored on a monthly basis by the Trust Board who will take such actions as necessary to ensure that the Trust meets its obligations in this area.

In accordance with the Training Needs Analysis in Trust Policy HR53 Statutory and Mandatory Training, all staff have an individual responsibility to ensure that they undertake mandatory Data Security & Protection training. All training should be recorded within staff personal record, ideally in ESR.

The Statutory & Mandatory Training module will be reviewed on an basis by the Data Security & Protection Operational Group to ensure that it is current and up to date and meets the requirements set by NHS Digital.

6.15 **Communication**

DSP has a Communications Plan which monitors how DSP communicates to all staff. DSP will communicate via a Monthly Newsletter any issues; learning; improvements in process. The Newsletter will also be used to remind/update staff on their obligations in the area of DSP

6.16 **Clinical Alerts**

DSP will oversee the clinical alerts that appear on the Trust's electronic patient systems, alongside colleagues via the Clinical Alerts Group. This Group is responsible for ensuring that alerts are relevant, up to date and that they meet DSP requirements.

7. AUDITING AND MONITORING

This policy will be assessed against the NHS Digital information governance and security requirements (Data Security & Protection Toolkit) and alongside the DSP Governance Pack to assure the Trust that full DSP requirements are being met

7.1 Associated and Related Procedural Documents

Copies of the associated policies, process and guidance documents can be found on the Trust's Intranet (Policies page)

8. REVIEW

This Policy is subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content;
- Where other policies/strategies/guidance issued by the Trust conflict with the information contained herein;
- Where the procedural or guidance framework of the NHS evolves/changes such that revision would bring about improvement;
- The review date has elapsed;

APPENDIX 1: TRAINING NEEDS ANALYSIS

All Data Security & Protection training is to be completed on an annual basis in line with the Data Security & Protection Toolkit. Completion of specialist training is required for job-specific roles within the Trust and is required to be undertaken every 3 years (for example staff handling subject access requests; caldicott guardian; SIRO, information asset owners; information asset administrators and HR staff handling subject access requests). Specialist Training will be provided in accordance with job role

The required training is detailed below:

Job Role	Mandatory Training (Annual Requirement)	Access to Records Management (Every 3 years)	Caldicott/SIRO Training* (Every 3 years)	Information Asset Owner/Information Asset Administrator Training (Every 3 years)	Cyber Security Training (Every 3 years)
SIRO	✓		✓		
Caldicott Guardian	✓		✓		
Data Protection Officer	✓	✓			✓
Information Asset Owners	✓			✓	✓
Information Asset Assistants	✓			✓	✓
Data Security & Protection Manager	✓	✓			✓
Data Security & Protection Team	✓	✓			✓
Subject Access Team	✓	✓			
All Staff	✓				

APPENDIX 2 – Data Security & Protection Governance Framework