Policy Document

Reference: DSP18

Over-arching Data Security & Protection

Version:	**11**
Date Ratified:	**March 2024 by the Executive Digital and Data Security & Protection Group**
Date of Next Review:	**March 2027**
Policy Author:	**Data Security & Protection Manager (Projects)**
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
10.1	November 2021	Page 5 - Inclusion of requirements for Chaplaincy/Pastoral Care Page 5 – inclusion of reference to Trust Privacy Notice Page 6 – inclusion of chaplaincy in Roles & Responsibilities and clarification of staff responsibilities with regard to accessing their own/friends' records
11	March 2024	Review Multiple – updating GDPR to UKGDPR Page 5 – updating Board Committee information Page 5 - updated roles & responsibilities Page 6 – updated/reinforced staff accessing records advice Page 7 – updated DPIA information to include DTAC Page 7 – updated ISA information Page 7 – updated information about the Cyber Team Page 7 – updated Advice/Guidance section Page 8 – updated Asset Management section Page 9 – updated the Training Section Page 9 – updated the Audit/Monitoring section Page 10 – updated the TNA Page 11 – updated the Governance Framework

Statement on Trust Policies

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

Equality Impact Assessment (EIA)

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Analysis Form is designed to help consider the needs and assess the impact of each policy. To this end, EIAs will be undertaken for all policies.

Does this policy have the potential to affect any of the groups listed below differently - please complete the below. Prompts for consideration are provided, but are not an exhaustive list

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	**Actions taken to mitigate negative impact** *(e.g. what action has been taken or will be taken, who is responsible for taking a future action, and when it will be completed by – may include adjustment to wording of policy or leaflet to mitigate)*
Age	No		
Gender	No		
Race	No		
Religion & Belief	No		
Sexual orientation	No		
Pregnancy & Maternity	No		
Marital status/civil partnership	No		
Gender Reassignment	No		
Human Rights	No		
Carers	No		
Socio/economic	No		
Disability	No		
Are there any adjustments that need to be made to ensure that people with disabilities			**No**

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	**Actions taken to mitigate negative impact** *(e.g. what action has been taken or will be taken, who is responsible for taking a future action, and when it will be completed by – may include adjustment to wording of policy or leaflet to mitigate)*
have the same access to and outcomes from the service or employment activities as those without disabilities? (e.g. allow extra time for appointments, allow advocates to be present in the room, having access to visual aids, removing requirement to wait in unsuitable environments, etc.)			
Will this policy require a full impact assessment and action plan? (a full impact assessment will be required if you are unsure of the potential to affect a group differently, or if you believe there is a potential for it to affect a group differently and do not know how to mitigate against this - please contact the Corporate Governance Department for further information)			**No**

CONTENTS **Page**

1. INTRODUCTION

This overarching Data Security & Protection Policy defines the Trust's operational approach to meeting the Data Protection legislation and national guidance 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 Overarching 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 limited 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. As stated above, 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 DSPAF.

4.1 Key Legislation

- Data Protection Act 2018 and the UK 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
- NHS Chaplaincy Information Governance Guidance

4.3 Key Standards

- NHS Data Security and Protection Toolkit
- Cyber Essentials Plus
- ISO 27001
- Information Governance Alliance (available via the NHS England Data Services website)
- 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 Transformation and People Committee will be updated on DSP issues via the Executive Digital and DSP Group, detailed in highlight report,

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for DSP 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 UK GDPR and DPA. The post holder is responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the data security & protection agenda. The post holder 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 the Records Service Operational Group which ultimately reports to the Executive Digital and Data Security & Protection 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 Team
The Trust's Data Security & Protection Managers are responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda, including the maintenance of an accurate and up to date Privacy (Fair Processing) Notice, management of the Trust's Records Management operations as well as overview of the Trust's Information Assets and generally supporting the Head of DSP in the delivery of the DSP agenda.

Executive Digital and Data Security & Protection Group (EDDSP)
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.

Operational Groups
The Data Protection Officer chairs the Trust's Operational Groups (Data Security & Protection Operational Group; Cyber Security Operational Group and the Record Services Operational Group – all responsible for overseeing key aspects of the Data Security & Protection Framework and the Executive Group Governance Pack provides further detail). This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework.

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 the Trust, 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 Workforce Information
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).

UHNM Chaplaincy
Will work with Information Services to identify patients who may require chaplaincy/pastoral care, maintain NHS Confidential Code of Conduct and adhering to the requirements of the Data Protection Act (2018).

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.

Staff should be aware that it is a criminal offence to access data (S.170 of the DPA 2018) without a valid business reason to do so, and that includes accessing staff's own records or those of family and friends, even with consent. The Trust views such actions as gross misconduct and disciplinary action, according to Trust procedures, will always be taken if such access is identified as the result of regular audits undertaken on Trust systems.

Transformation & People Committee
The Transformation & People 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 DSPAF are outlined below.

6.1 **Data Protection Impact Assessments**

The DSP team is responsible for ensuring full due diligence is undertaken which includes, but is not restricted to, data protection impact assessments (carried out whenever there is a change that is likely to involve a new use or significant change the way in which personal and special categories of personal data is handled) and the Digital Technology Assessment Criterial (undertaken by the supplier when the Trust purchases digital software to ensure that it meets our standards).

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 agreements are in place with our partner organisations and other external organisations access UHNM data – such as Information Sharing Agreements; Data Processor Agreements and Non-Disclosure Agreements.

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.

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 People Directorate 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 Lead and Communications Team, in 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 Record Service Operational Group.

6.9 **Information/ Cyber Security**

The DSP team will provide relevant guidance on information security standards and practices working closely with the Cyber Team on aspects of cyber security.

6.10 **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.

6.11 **Advice and Guidance**

The DSP Team is responsible for oversight of the DSP Toolkit which is an annual submission made and which provides assurance for the Trust's data security & protection practices. As part of its oversight role, the DSP team, will provide subject matter advice where required, including a regular DSP Newsletter which highlights relevant advice and guidance.

6.12 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.

Asset Management is also key when the Trust engages with external contractors who are supporting on projects and services or where there is no digital system in place.

6.13 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.

6.14 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.

6.15 Training

Mandatory Data Security & Protection training for all staff (whether permanent, temporary or contracted) is included in the Trust's 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 three-yearly basis as per the requirements of the relevant Policies

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.

In accordance with the Training Needs Analysis in Trust Policy HR53 Statutory and Mandatory Training and contract, 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 annual 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 England

6.16 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

7. AUDITING AND MONITORING

Each of the Operational Groups (outlined above) has a defined business cycle. As part of this programme of work, key reports are presented to the Operational Groups to provide assurance against the DSP framework.

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:

	Caldicott Guardian	**SIRO**	**Information Asset Owners/ Administrators**	**Data, Security & Protection Team**	**Subject Access Request Team**	**Corporate Records Champions**	**All Staff**
DSP Mandatory Training (Every 3 years): • Confidentiality: • Information Security • Records Management	√	√	√	√	√		√
Caldicott Training (Every 3 years)	√						
SIRO Training		√					
Information Asset Training (Every 3 years)			√				
Access to Records (Every 2 years)				√	√		
Corporate Records Training (Every 3 years)						√	

APPENDIX 2 – Data Security & Protection Governance Framework

IM&T

- DSP14 - Registraton Authority Policy
- IT02 - Personal Information Security and Acceptable Use Policy
- IT01 - Information Security Policy
- IT12 - Data Back Up Policy
- IT13 - User Access Management Policy
- IT09 - Secure Disposal Policy(s)
- IT10 and IT11 - Firewall Build Policy(s)
- IT15 - Update & Patching Policy
- IT10 - Corporate Logging Policy
- IT16 - Anti-Virus Policy
- IT19 - Secure Development & System Engineering Policy
- IT16- Device Type Service Policy
- IT17 - Password Management Policy
- IT18 - Vulnerability Mgt Policy
- Cyber Incident Response Plan/ Incident Recovery
- Starts, Movers & Leavers SOP
- Cyber Supporting SOPS e.g.

  AD/Logging/Firewall Logging
  Investigating Phising Emails - Infrastructure Process
  Cyber User Access
  Mobile & Removable Devices (Remote Working)
  Cyber IM&T Incident Response Processes
  IM&T Incident Recovery
  (Please check the Intranet for details of SOPs)

Learning & Assurance

- RM07 - Incident Management Policy
- RM01 - Risk Management Policy
- HR53 - Statutory & Mandatory Training Policy
- G15 - Clinical Audit Policy
- RM09 - Analysing & Learning Policy)
- DSP Handbook

Data Security & Protection

- DSP 10 - Data Protection & Confidentiality Policy
- DSP15 - Asset Management Policy (inc. Privacy by Design)
- C27 - Data Quality Policy
- G21 - Managing Visits by Celebrities, VIPs and other Official Visitors to UHNM
- DSP18(S1) - DSP Audit SOP (including Corporate Records and Confidentiality Audit)
- DSP10(S2) - Explicit Consent
- DSP15(S1) - Third Party Governance SOP
- DSP15(S2) - DPIA
- DSP10(S1) - Pseudonymisation & Electronic Use of PID SOP
- DSP10(S2) - Explicit Consent
- DPA Act 2018
- FOI Act 2018
- Access to Health Records Act 1990
- NHS Confidentiality Code of Conduct
- National Data Guardian Review 2016
- DSP Induction Booklet
- Clinical Alert Owners Handbook

Records Management

- DSP16 - Corporate Records Management & Information Lifecycle Policy
- RE01 Multi-Disciplinary Health Records Policy
- RE02 - Clinical Photographic & Video Policy
- DSP16(S1) - Version Control SOP
- NHS Records Management Code of Practice

Legal

- DSP08 - Freedom of Information Policy
- DSP17 - Access to Personal Information (SAR Policy)
- DSP17 (S1) - SARs Sop
- DSP17 (S2) - Law Enforcement Requests SOP
- DSP18(S2) - Handling Objections to Processing
- DPA Act 2018
- General Data Protection Regulations 2018
- FOI Act
- Access to Health Records Act 1990

LSMS

- EF20 - CCTV Policy
- EF02 - Security Policy
- ICO CCTV Code of Practice
- Surveillance Camera Code of Practice

IM&T Policies | SOPs | Other Divisions' Policies | Guidance | DSP Policies