Policy Document

Reference: DSP15

University Hospitals of North Midlands NHS Trust

Information Asset Management – incorporating Data Protection by Design

Version:	**2.2**
Date Ratified:	**November 2021 Executive Data, Security and Protection Group**
Minor Amends:	**March 2023 / June 2024**
To Be Reviewed Before:	**November 2024**
Policy Author:	**Information Security Manager**
Executive Lead:	**Senior Information Risk Owner**

Version Control Schedule

Version	Issue Date	Comments
1	November 2020	New policy intended to better support the DSP toolkit and an ensure UHNM is fulfilling its responsibilities in relation to information assets, their procurement and management throughout the information asset management lifecycle.
2	November 2021	Corrections to formatting and expansion of definitions Update to flow diagram in appendix 4 to remove IG reference
2.1	March 2023	Policy updated to include information around the management of AI software **Page 4 ~ Information added "**The use of new technologies and advances in technology such as Artificial Intelligence (AI) has the potential to provide a number of benefits to health and care and while there is a wide ranging potential in the pace of this development, it is important that its implementation and usage is monitored and provided in a way that upholds both national standards and local policy. This is achieved through the demonstration that there is a strategy for planning the implementation and use of machine learning algorithms, including a discrepancy workflow and feedback process, and the completion of DCB0160 documentation and adherence to any national standards associated with the technology. **Page 5 ~ Information added "Artificial Intelligence (AI)** – AI is the use of digital technology to create systems capable of performing tasks commonly thought to require human intelligence" **Page 9 ~ Information updated "**The DPIA must also include where applicable information regarding any AI technology used and how this will be developed in line NHS England guidance. **Page 11 ~ last paragraph from "**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" **to read "**The Statutory & Mandatory Training module will be reviewed on an annual basis to ensure that it is current and up to date and meets the requirements set by NHS Digital". **Pages 6 & 7 ~** All references regarding the Information Governance Group meetings and Data Security and Protection Steering group to read Executive Digital and Data Security & Protection Group meeting. **Page 11 ~** spelling mistake of stuatory to statutory.
2.2	June 2024	**Page 10 ~** Information added to cover the Record of Processing (ROPA).

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

Information handling can represent a significant corporate risk in the sense that failure to protect information properly or use it appropriately can have a damaging impact on the Trust's reputation with patients, customers, the public and other public sector bodies. It also opens up the possibility of legal action against the Trust and its board under its duty of care to handle patient information appropriately.

The risks associated with information assets are inherent in all administrative and business activities and everyone working for or on behalf of UHNM must continuously manage information assets. The Trust recognises that the aim of information asset management is not to eliminate risks, but rather to provide the structural means to identify, prioritise and manage the risks involved in all UHNM activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that would be derived.

The key requirement is for information assets to be managed in a robust way within work areas and not be seen as something that is the sole responsibility of Information Management and Technology (IM&T) or Data Security and Protection (DSP) staff. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing Data Security and Protection framework within which UHNM is already working. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

Information asset management is an integral part of good management practice. The intent is to embed information assets management in a very practical way into business processes and functions. This is achieved through key approval and review processes/controls, and not to impose assets management as an extra requirement.

The use of new technologies and advances in technology such as Artificial Intelligence (AI) has the potential to provide a number of benefits to health and care and while there is a wide ranging potential in the pace of this development, it is important that its implementation and usage is monitored and provided in a way that upholds both national standards and local policy. This is achieved through the demonstration that there is a strategy for planning the implementation and use of machine learning algorithms, including a discrepancy workflow and feedback process, and the completion of DCB0160 documentation and adherence to any national standards associated with the technology.

2. SCOPE

This Policy is to provide a clear Information Asset Management Framework that has effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. This policy sets out the arrangements that University Hospitals North Midlands NHS Trust has in place to secure its information assets

3. DEFINITIONS

Information Assets – is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles, for example the trust PAS system; the Network structure or the trust clinical correspondence system (iPortal). Identified Information Assets are formally recorded on the Information Asset Register.

Software Assets – relates to off the shelf purchased software i.e. Adobe / MS Office.

Threat – any event or situation which has the potential to cause the loss of, unauthorised access to, unauthorised changes or destruction of, information assets held or controlled by UHNM.
Event – a threat which materialises.

Risk – the likelihood and severity of an event occurring. Other words, such as probability, consequence or impact are sometimes used instead, but UHNM uses likelihood and severity in all documents to avoid confusion.

Severity – The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Likelihood – A qualitative description or synonym for probability or frequency.
Information Assets Assessment – the systematic process for prioritising information assets on the basis of a combination of the severity of consequence and likelihood of occurrence.
Information Assets Management - the systematic process for identifying, assessing, mitigating and reviewing information asset risks.

Controls – documents, systems, processes, devices and equipment intended to mitigate the likelihood and/or severity of a risk.
Information Incident – any event which results, or might have resulted, in the loss of, unauthorised access to, or unauthorised changes or destruction of, any information assets held or controlled by UHNM.

Reportable incident - An incident that is 'likely' to have caused 'minor harm' is reportable to the ICO.
General Data Protection Regulation – The General Data Protection Regulation (GDPR) applies across Europe from 25th May 2018. GDPR supersedes the previous UK Data Protection Act 1998 (DPA). GDPR brings significant and wide-reaching changes in the way we deal with data protection. It expands the rights of individuals to control how their personal data is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

Data Protection Act 2018 – supersedes the DPA 1998.

Artificial Intelligence (AI) – AI is the use of digital technology to create systems capable of performing tasks commonly thought to require human intelligence.

4. 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 Executive Digital and Data Security & Protection Group.

Information Asset Owners (IAO)
IAOs are directly accountable to the SIRO and must provide assurance that information assets are being managed effectively in respect of the information risks that they are responsible for.

IAOs are responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. This will include:

- understanding UHNM's plans to achieve and monitor the right Data Security & Protection culture, across Trust and with its business partners;
- taking visible steps to support and participate in that plan, (including completing own training);
- ensuring that staff understand the importance of effective Data Security and Protection and receive appropriate education and training;
- considering whether better use of any information held is possible, within applicable Data Security and Protection rules, or where information is no longer required.

IAOs are responsible for knowing what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset. This will include:

- maintaining an understanding of 'owned' assets and how they are used;
- approving and minimise information transfers while achieving business purposes;
- approving arrangements where it is necessary for information to be put onto portable or removable media such as laptops and USB pens and ensure information is effectively protected to NHS Data Security and Protection standards and comply with Trust policies;
- approving the information disposal mechanisms for the asset in line with Trust Policy;
- ensuring that all new data (information) flows are recorded on spread sheets and risk assessed via Datix when a new flow is established/identified,
- ensuring data (information) flow mapping exercise is carried out for all assets at least annually, and that such data maps are provided to the Data Security and Protection Manager and Data, Security and Protection Operational Group when required.
- training and education in relation to machine learning algorithms.

IAOs are responsible for knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy.
This will include:

- understanding UHNM's policies on the use of information and the management of information assets;
- ensuring decisions on access to information assets are taken in accordance with NHS Data Security and Protection good practice and the policies of UHNM;
- ensuring that access provided to an asset is the minimum necessary to satisfy business objectives;
- ensuring that the use of the asset is audited regularly and that use remains in line with policy;
- ensuring that all new assets are subject to a Data Privacy Impact Assessment (DPIA) (where appropriate), recorded on the Information Asset Register and risk assessed when a new asset is acquired/identified;
- ensuring that an Information asset register is maintained and made available to the Data Security and Protection Manager and Data, Security & Protection Operational Group whenever requested.

IAOs are responsible for understanding and addressing risks to the asset, and providing assurance to the SIRO. This will include:

- seeking advice from Data Security and Protection subject matter experts when reviewing information assets;
- conducting Data Protection Impact Assessments for all new projects that meet the criteria specified by the Information Commissioner; this is a legal requirement under GDPR;
- undertaking quarterly asset assessment reviews for all 'owned' information assets in accordance with NHS Data Security and Protection guidance and report to the Data Security and Protection Manager, ensuring that information assets are identified, documented and addressed, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks;
- escalating risks to the Data Security and Protection Manager and/or SIRO where appropriate and to make the case where necessary for new investment to secure 'owned' assets;
- providing an annual written assessment to the Data Security and Protection Manager for all assets 'owned' by them, following guidance from the Data Security and Protection Manager on assessment method, format, content, and frequency.

IAOs will, with support from IM&T and 3rd party support organisations where appropriate, ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and take action to mitigate against any reasonably anticipated threats or hazards to the security or integrity of such information. IAOs may nominate Information Asset Assistants (IAA)

Information Asset Administrators (IAA)

IAAs are directly accountable to the IAO of the asset and must provide assurance that information assets are being managed effectively in respect of the information asset that they 'administer'. IAAs will:

- ensure that policies and procedures are followed in respect of Data Security and Protection and information asset management;
- recognise actual or potential security incidents and consult their IAO on incident management;
- ensure the confidentiality, integrity, and availability of all information that their asset creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- ensure Information Asset Registers are accurate and up to date;
- ensure the Data Flow Mapping information is accurate and up to date;
- support the completion of the Data Security and Protection toolkit and any such associated work

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.

Executive Digital and Data Security & Protection Group (EDDSPG)
The Caldicott Guardian and the SIRO are the joint chairs of the Trust's EDDSPG. 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 Head of DSP/Data Protection Officer is the chair of 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 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 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.

5. INFORMATION ASSET MANAGEMENT PROCESS

Protection of Assets
UHNM will be particularly careful to protect all data where the release or loss of could cause:

- Harm or distress to patients or staff;
- Damage of UHNM's reputation;
- Financial loss or exposure to UHNM;
- Major breakdown in information systems, information security or information integrity;
- Significant incidents of regulatory non-compliance.

Information asset register
UHNM will establish and maintain a corporate Information Asset Register by Division. This register will:

- be managed by the DSP team. There is however no intention of replicating information already on other asset registers if directorates hold these, so references can be made where appropriate to other key registers; e.g. Staff list and skill sets held within ESR, IT asset register of equipment and software assets, clinical technology register etc.;
- record/log the documentation suite for each asset which is to be maintained by IAOs and IAAs the DSP team can provide advice and guidance
- Will be overseen by the Data Security and Protection Manager, who will review to ensure that all IAOs regularly update their asset records.

Information Asset assurance in the information asset lifecycle

Data Protection by design, DPIAs

It is a legal requirement under GDPR that 'Data Protection by design' is established; this means that all Data Protection requirements are to be considered prior to implementation of any new system/service, or before any significant changes in existing systems / services are made. As such, it is a legal requirement that a Data Protection Impact Assessment (DPIA) is conducted for all new projects and for any changes to existing systems/processes, (for example new systems, new services, any change in how the service is run, any change in how information is collected and/or recorded, when a request is received to share information on a regular basis, a request to send a questionnaire to patients, etc.).

- In the first instance a DPIA screener form can be completed – which the DSP team will review to confirm whether a full DPIA is required.
- This will be undertaken in accordance with guidance available on the Data Security and Protection intranet section
- Using the DPIA form and guidance documents available from the Data Security and Protection team, which includes both a risk assessment and data flow element that must also be completed. The DPIA must also include where applicable information regarding any AI technology used and how this will be developed in line NHS England guidance.
- Approval for DPIAs in the first instance will be from the Trust Data Protection Officer. Where a risk that is deemed 'high' or 'unmitigated' or where other concerns are identified this will be escalated to the SIRO for consultation and review. Where a risk continues to be high or unmitigated the DPO will review for to determine whether it needs to be reported to the ICO, which is a requirement under the terms of our registration. *This will occur if the Data Security and Protection Manager feels there is still a risk to the organisation or data subjects that has not been mitigated or taken in to consideration during the DPIA process.

Supplier and 3rd Party governance

Where a new or changed system / project or development has been identified as containing identifiable or otherwise sensitive data, and a 3rd party which will be engaged in any of the below;

- Provide hosting facilities
- Provide support either on site or remotely
- Provide processing services

then a Mandatory pre tender questionnaire must be completed by the 3rd party to provide assurance of their data protection and security processes and culture. On return this will be reviewed by the DSP team, in conjunction with the completed DPIA – to give a 360o view of the project as a whole.

Any contracts should contain standard NHS terms and conditions (including Schedule 3 which deals with information and data provisions). Where relevant clauses are not included then the GDPR addendum should be added. See Appendix 3

All contracts should be regularly reviewed against the SOP DSP15(s1) Third Party Governance Requirements

3rd Party Governance Requirements

General policy requirements are described in this section and shall be reflected in Trusts Over Arching DSP policy DSP18, procurement processes and contract negotiations.

- The Trust will identify threats, vulnerabilities and risks within the supply chain by carrying out appropriate risk assessment and management.
- The Trust will implement relevant mitigations to counter identified threats, vulnerabilities and risks within the supply chain.

- The Trust shall ensure that relevant staff are trained as appropriate in the security requirements of the supply chain.
- The Trust shall ensure that security requirements, including security incident response, are included in every contract in line with all relevant Trust security policies.
- The Trust must ensure that the security aspects of all supplier contracts are closely managed and monitored.
- The Trust must ensure that contracts include provisions that any breach of security or security requirements by the supplier may lead to an immediate termination of the contract.
- In line with GDPR Requirements, a Data Protection Impact Assessment (DPIA) must be carried out before any access granted or service provided to determine if personal data will be impacted.

See DSP15(S1) 3rd Party Governance Requirements SOP for additional information this includes details of:

- Requirement for 3rd party access to Trust systems including remote access
- System used to provide access
- Supplied hardware and software
- 3rd party service requirements
- Physical access
- Reporting requirements

Information asset assurance

Where a DPIA is approved – relating to an information asset there will be a suite of documentation generated to provide assurance – this will be accessed and managed through the IAO Portal. This documentation is reviewed at least annually.

- System Level Security Policy (SLSP)
  - Required in all cases
- Data flow assessment
  - Required in all cases
  - Forms part of the SLSP document and DPIA for new systems / services
- Business Continuity and Disaster Recovery
  - Required in all cases but can be cross referenced to existing documentation if suitable
- Risk assessment
  - Required in all cases
- Record of Processing (ROPA)
  - Required in all cases
  - Will be reviewed every 6 months to ensure that the information is accurate
- Sharing and Processing Agreement
  - Required where details are not sufficiently captured in a legally binding contract

Depending on the nature of any risks identified additional assurance documentation may be required.

Check list for depreciated assets

When an information asset is deemed to be no longer required the following must be confirmed by the IAO

- Is there any retention requirement for the data and how long
- Where will any retained data be stored
- Who will be the custodian of this data to preserve its integrity
- Will data be transferred to another system
- Is there a replacement for this system
- If the data is to be deleted is a destruction certificate available – or deletion confirmation if in house

A depreciated asset will be presented to the asset management working group for recording and assurance that the data has been suitably retained, stored or deleted as appropriate. Once the group is happy, the assurance documentation will be retained for audit purposes and the system will be noted as excluded from review in the asset database with a suitable comment. The asset will then be removed from the IAO portal.

Privacy Notice

When a new DPIA is approved by the DPO the Trust Privacy notice must be reviewed for any necessary changes to be made – this will be reviewed by the Trust Data Security and Protection Manger.

6. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

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 requires 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 of policy DSP18.

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 has 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 to ensure that it is current and up to date and meets the requirements set by NHS Digital.

7. MONITORING AND REVIEW ARRANGEMENTS

Monitoring Arrangements
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

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;

8. REFERENCES

SOP – DPIA
SOP – 3rd party access management
SOP – adding an information asset to the IAO Portal (DSP TEAM ONLY)

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

9. APPENDICES

Appendix 1 - Examples of risk for information assets

1. Information Asset not available:
   a. Theft of information
   b. Loss of information
   c. Information corrupted/unreadable/virus
   d. Information incorrectly disposed
   e. System/network failure Backup of information not in place
   f. Information unusable – contaminated, e.g. water, smoke, fire, asbestos dust
   g. Wilful damage by employee/public

2. Information accessed by unauthorised person
   a) Passwords shared
   b) No password protection
   c) Mobile media not encrypted
   d) Information disclosed by accident
   e) Physical security not in place, e.g. Locks on doors, cabinets, drawers
   f) Eavesdropping
   g) Information available on a public drive/shared drive
   h) Insecure disposal of information
   i) System misused/hacked
   j) Contractors, temps, students not authorised users

3. Other risks
   a) Information used for other purposes than originally collected, no consent given. (secondary uses of personal information)
   b) Information out of date
   c) Information kept longer than retention period
   d) No licence for software therefore using illegally, may have illegally downloaded
   a) Loss of expertise for a specific information asset if only one member of staff trained in use for example
   e) Procedures not in place for use of information asset
   f) Staff not trained in use of Information Asset, include contractors, temps students etc.
   g) Booking out system not in place for paper documentation/files/records
   h) Uncontrolled copying of information
   i) Version control not in place
   j) Duplicated information

Appendix 2 - Examples of Controls that may Reduce Risk

1) Relevant policies are in place and are being followed e.g. security policy, safe haven, mobile media.
2) Confidentiality and other IG policies such as Email and Internet Policy are read and understood by staff.
3) Job descriptions include Information Security and IG responsibilities where necessary e.g. for IG Manager, SIRO, Information Asset Owners.
4) HR screening undertaken as per HR policy in particular where access to sensitive data is required.
5) Staff is made aware of the confidentiality/IG clause in their contract of employment.
6) Procedures and protocols in place and being followed by staff who are regularly trained.
7) Ensure all staff undertakes annual IG Training.
8) Ensure security weaknesses and software malfunctions reported.
9) Ensure actions taken following reported incidents to learn from mistakes made.
10) Undertake regular risk assessments of buildings/areas where information is held to ensure area is secure including key management for access to building.
11) Clear desk policy for personal/confidential information.
12) Ensure workstations locked/turned off by user when not in use. Laptops must be removed from desk/docking station by user at end of working day and locked away securely.
13) Password protected screensaver should be in use by all staff.
14) Prohibit working in public areas if possible; assign secure working areas that cannot be accessed by public if possible to prevent tampering with equipment or viewing of information.
15) Site workstations/laptops where they cannot be overlooked by unauthorised personnel. Obtain privacy screens if necessary.
16) Equipment taken off site – ensure staff aware of procedures in Mobile Media Security Policy to ensure laptops etc. are kept secure at all times and not left in cars/unattended for example.
17) All mobile media must be encrypted as per Mobile Media Security Policy.
18) Ensure confidential waste, IT equipment; fax rolls and records are destroyed in accordance with Trust Policy (e.g. Records Management Policy and the Mobile Media Security Policy)
19) Business Continuity plans in place and tested to protect information assets.
20) Data Protection Impact Assessments completed for new/changed processes/systems where information may be used in a different way than was originally collected for.
21) Ensure information sharing agreements in place where information needs to be shared with other organisations.
22) Specialist Security Information Advice provided by IG Team.
23) Third party assurances obtained regarding information security e.g. completion of DS&P Toolkit, clause in contracts.
24) Up to date Inventory of information assets. An inventory is a detailed list of what information is held. E.g. a filing cabinet may hold ‘Payroll Records’ as reported on the Information Asset Register, the inventory will list the actual record held in the filing cabinet.
25) Correct classification and marking of information as to whether it is personal, sensitive, corporate or confidential etc. So it is clear to users what type of information is held.
26) 26. Information should be held on network drives, no personal information should be ‘stored’ indefinitely on mobile media such as pen drives, cd’s, laptop hard drives (these can be used for transfer of information only)
27) 27. Secure backups and audit trails in place for system.
28) 28. Keep track of who has access to restricted drives. Users should be deleted when they leave or transfer to another department
29) 29. Exit strategies for staff leaving, suspended or made redundant to ensure access to systems prohibited, IT equipment and keys handed back to manager.

Appendix 3 – GDPR Contract Insert

Description	Details
Identity of the Controller and Processor	
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of Personal Data	
Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete unless requirement under union or member state law to preserve that type of data.	

Appendix 4 - Data protection by design