South London and Maudsley
NHS Foundation Trust

Information Governance Policy

Version:	7
Ratified By:	Information Security Committee
Date Ratified:	May 2019
Date Policy Comes Into Effect:	August 2019
Author:	Head of Information Governance
Responsible Director:	Chief Information Officer (SIRO)
Responsible Committee:	Information Security Committee
Responsible Committee Approval Date:	May 2019
Target Audience:	All Trust Staff
Review Date:	May 2021

Equality Impact Assessment	Assessor: Deputy IG Lead	Date: 15/08/2019
HRA Impact Assessment	Assessor: Deputy IG Lead	Date: 10/03/2019

Document History

Version Control

Version No.	Date	Summary of Changes	Major (must go to an exec meeting) or minor changes	Author
5	01.11		Major changes A review of the Information Governance Policy against recent organisational changes and changes in information governance Standards.	M Soncul
5.1	03.13		Minor changes	M Soncul
6	08.15		Minor changes	M Soncul
7	September 2018	Policy rewritten to reflect new Data Protection Act 2018 and General Data Protection Regulation (GDPR)	Major	Deputy IG Lead
	March 2019	Updated with policy around correspondence with patients	Minor	Head of IG

Consultation

Stakeholder/Committee/ Group Consulted	Date	Changes Made as a Result of Consultation
Head of IG / DPO Officer	October 2018	Policy rewritten to reflect GDPR requirements
Information Security Committee	October 2018	No change
Information Security Committee	March 2019	Updated with section on correspondence with patients

Service Users/Carers consulted	Date	Changes Made as a Result of Consultation
Caldicott Committee	October 2018	No change

Plan for Dissemination of Policy

Audience(s)	Dissemination Method	Paper or Electronic	Person Responsible
All staff	Online,	Electronic	Policy Co-ordinator

Key changes to policy:
Updated with detail on correspondence with service users and DPIAs

Plan for Implementation of Policy

Details on Implementation	Person Responsible
Compliance with new Data Protection Act 2018 and General Data Protection Regulation (GDPR)	All staff
Data Security	Chief Information Officer

Contents

1. Policy Summary

1.1 South London and Maudsley NHS Foundation Trust (The Trust) is committed to providing world-class and efficient mental health and substance misuse services in a new landscape. This new landscape has highlighted the need to organise and regulate the compound use of clinical and corporate information.

1.2 It is of paramount importance to ensure that clinical and corporate information is effectively managed whilst utilised to their maximum potential to benefit service users and the public. The effective management of information requires appropriate policies, procedures, management accountability and structures to provide a robust governance framework.

1.3 All staff, whether permanent, temporary or contracted are responsible for ensuring that they comply with information governance standards.

1.4 The Trust supports the principles of Corporate Governance and recognises its public accountability, but equally places importance on confidentiality of personal confidential data, commercially sensitive information and the security arrangements to safeguard sensitive information.

1.5 The legal obligations for data protection, information sharing, disclosures, subject access and service user rights to confidentiality are outlined in the Trust Confidentiality Policy. A separate Human Resources Data Protection Policy is implemented for the protection of staff information.

1.6 The Caldicott Guardian is responsible for protecting patient information and the Senior Information Risk Owner (SIRO) is responsible for information risk.

2. Introduction

2.1 Reliable information is a fundamental requirement in the NHS. Good quality information in healthcare services is crucial for:

- Clinicians to make decisions about patient care,
- Clinical management to decide which services to provide and commission,
- Services to monitor performance management and plan improvements,
- Infrastructure management to use support services effectively,
- Public to be reassured that resources are being used wisely,
- Patients to make choices about how and where they want to get treatment

2.2 What is Information Governance (IG)?

Information Governance (IG) is a term that is used to describe how organisations and individuals manage the way information is handled within the health and social care system in England. It covers the requirements and standards that the organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

2.2.1 IG encompasses information security, information risk management, patient and staff confidentiality, information sharing, clinical and organisational records management, data quality, secondary uses of information and freedom of access to public information. Good information management is the organisational ability to protect personal confidential data, use this information effectively and ethically for the purposes the information was collected.

2.2.2 Information Governance ensures compliance with the new **Data Protection Act 2018 (DPA18), General Data Protection Regulation (GDPR)** the Freedom of Information Act (2000), the Human Rights Act (1998), Common Law Duty of Confidentiality and best practice when handling personal, sensitive and Business information.

2.2.3 It also allows staff to ensure that personal information is dealt with lawfully, fairly, securely, efficiently and effectively to deliver best possible care. While doing so, the Trust Information Governance Framework will support staff, protect patients and enhance working in partnership to maintain the leading role in mental health service delivery.

2.2.4 The Trust is working in partnership under an Academic Health Sciences Centre (AHSC). King's Health Partners, which is bringing together leading organisations (three NHS Foundation Trusts and a higher education institution), will have significant dependency on information assets that is generated by partners in the course of their business. The partnership has further highlighted the need to organise and regulate the compound use of clinical and corporate information.

3. New legislation

3.1 Data Protection Act 2018 (DPA18) and General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) was approved in 2016 and has become directly applicable as law in the UK from 25th May 2018.

3.1.1 The Data Protection Act 2018 (DPA18) is the UK's implementation of the General Data Protection Regulation (GDPR)

3.1.2 DPA18 fills in the gaps in the GDPR, addressing areas in which flexibility and derogations are permitted. The GDPR will not be directly applicable in the UK post Brexit but the DPA18 will ensure continuity by putting in place the same data protection regime in UK law pre- and post-Brexit, equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

3.1.3 DPA18 does not repeat all the provisions of the GDPR but cross-refers to the relevant provisions as appropriate. When the GDPR and DPA18 came into force, it will therefore be necessary to view the DPA18 and the GDPR side by side in order to see the complete picture of all the data protection legislation.

3.1.4 The Trust IG policy and policies under the IG framework refer to relevant provisions of the DPA18 and GDPR. These policies will also be kept up to date in light of any relevant guidance issued from Government and the Information Commissioner's Office (ICO).

3.2 Legal Use of Information

Under DPA18 and GDPR, the Trust must establishing a lawful basis for processing all personal data. The Trust must also publish the lawful basis it relies on for processing personal data. The published notice can be found on the Trust website https://www.slam.nhs.uk/about-us/privacy-and-gdpr.

3.2.1 South London and Maudsley NHS Foundation Trust, as a health care provider, is subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about service users for their direct care. This duty is subject to both the common law duty of confidence, DPA18 and GDPR. For common law purposes, sharing information for direct care is on the basis of implied consent, which may also cover administrative purposes where the patient has been informed (Via fair processing notice and conversation with care team) or it is otherwise within their reasonable expectations.

3.3 Common Law Duty of Confidentiality

Confidentiality requirements are unaffected by the new laws. The fact that consent may be obtained for confidentiality purposes does not mean that consent must also be the lawful basis applied for the purposes of processing data in compliance with the GDPR. Well established national guidance on confidentiality remains applicable. GDPR requirements do not affect the common law duty of confidence (confidentiality). The practice of assuming implied consent under patients' reasonable expectations of data sharing and processing for direct care purposes will continue to be valid for common law duty of confidentiality purposes.

3.4 Consent under new law

In the new DPA18 and GDPR, the definition of consent has been enhanced Article. 4(11). Consent must be given by a statement or by a clear affirmative action from the data subject. It must be freely given, specific, informed and unambiguous. The proposed processing under consent must be clearly distinguishable from other matters that are being consented to in written agreements.

3.4.1 There must be requirement to facilitate the withdrawal of consent. It should be as easy to withdraw as to give consent.

a. **Research legal basis and consent:** Consent is an important part of the research process and is frequently sought for participation in research studies. One reason is to ensure that any disclosure of confidential information meets the requirements of the common law duty of confidentiality. Where consent is sought from research participants, they are normally told how information about them will be used. Consent to participation in research is not the same as consent as the legal basis for processing under data protection legislation. Visit the https://www.hra.nhs.uk/ for more information and legal basis for research.

4. Definitions

4.1 **Information Governance** is the term used to describe how organisations and individuals manage and handle data within the health and social care system in England (the Information Governance Review, Department of Health 2013). In practical terms, Information Governance is about sharing information appropriately. There is a body of legislation that protects personal information shared in appropriately could mean a fine for the organisation or even prison for an individual.

4.2 **The General Data Protection Regulation (GDPR)** is European Union regulation that will come into force across 28 EU Member States, including the United Kingdom in May 2018.

4.2.1 The Regulation lays down rules relating to the protection of natural (living) persons with regard to the processing of personal data and rules relating to the free movement of personal data. It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

4.3 **Processing data**: The processing data includes doing any of the following to the data: collecting, structuring, altering, using, disseminating, combining, destroying, recording, storing, retrieving, making available, restricting, organising, adapting, consulting, transmitting, aligning and erasing

4.4 **Personal identifiable information (PII) or personal data:** Personal identifiable information constitutes any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. This information includes name, address, full post code, date of birth, NHS number and Trust ID, photographs, videos, audio-tapes or other images of service users, or anything else that may be used to identify a service user directly or indirectly. E.g. rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified

4.4.1 The new legislation requires the trust to apply stricter controls to person-level data as the data rows get longer and richer even when the data is de-identified.

4.5 **Common law duty of confidentiality:** A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is generally accepted that information provided by patients or service users to a health or social care service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. This is an important point, as once information is effectively anonymised it is no longer confidential.

4.5.1 Under English common law, information given in circumstances where it is expected that a duty of confidence applies (such as within the relationship between a patient and their health and social care professional) cannot normally be disclosed without that person's explicit consent. Confidential information may be shared within the care team where necessary for the direct care of that individual patient - which is the reason the information is held.

4.5.2 Any disclosure outside the care team must have one of the following in order to be lawful:

- The explicit, informed and freely-given consent of the patient.
- A legal duty to disclose (such as a statutory obligation or court order).
- A statutory basis to permit disclosure (such as Section 251 support).
- Exceptionally, an overriding public interest in disclosure which outweighs both the individual's own rights and freedoms and the public interest in a confidential health service (such as safeguarding disclosures).

4.6 **Duty to Share:** Health and adult social care providers and commissioners have a statutory duty to share information about individuals where such sharing is likely to facilitate the provision of care to that individual, and is in the individual's best interests. This duty only exists where such sharing would otherwise be lawful, under both the Data Protection Act 1998 and the common law duty of confidence. It does not, in and of itself, provide a lawful basis to share information.

4.7 **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be ‘no surprises’) and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. The Mental Capacity Act 2005 Code of Practice should be consulted with regards to decisions about capacity and competence.

4.8 **Direct care** is defined as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual). It includes:

- supporting individuals' ability to function and improve their participation in life and society;
- the local audit/assurance of the quality of care provided;
- the management of untoward or adverse incidents;
- the measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

4.8.1 It does not include research, teaching, financial audit, service management activities or risk stratification (see note below on borderline cases).

4.9 **Care Team** are the health and social care professionals who provide direct care to an individual patient and the administrative or other on-regulated staff with a legitimate relationship to the patient who directly supporting that care (such as by booking appointments). There are specific conditions which determine whether a non- regulated individual should be considered part of the care team but in practice the distinction is often obvious, based on the person's role and relationship to the patient.

4.10 **Data Protection and Privacy Impact Assessment (DPIA or PIA**): is a systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure. DPIA are a requirement under the General Data Protection Regulation

4.11 **Data breach:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

4.12 **Fair Processing:** Processing personal data "fairly" means doing so within the expectations of individuals. If patients would not reasonably expect to be using their data for a certain purpose, we must take steps to inform them about it in advance. The right to object to confidential information being shared for purposes beyond an individual's care and treatment should be followed through by actual processes to ensure individuals fully understand what they can object to and how to initiate that process, otherwise it could be considered unfair processing.

4.13 **NHS Digital Data Security and Protection Toolkit :** The data security and protection toolkit replaces the NHS information governance toolkit as an online self-assessment tool that enables health and social care organisations, commissioners, IT suppliers and other relevant third parties to determine how secure their data is. The toolkit enables organisations to report breaches. The guidance provided by the toolkit changes every year.

4.14 **Digital Services Asset:** Any information system, computer programme or other equipment owned by the Trust.

4.15 **Information Asset**: Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation

4.16 **Information Asset Owner:** The member of staff responsible for an information system in the Trust, i.e. any service specific software or information system.

5. Purpose and Scope of the Policy

5.1 The Information Governance Policy sets out the systems and processes in place to ensure the following principles:

- Information used by the Trust in undertaking its business is secure.
- Information is kept confidential where appropriate.

5.2 Transfer of information in bulk is secure with

- Availability of information for operational purposes is maintained within set parameters according to appropriate procedures.
- Integrity of information is developed, monitored and maintained to ensure it is of sufficient quality for use within the purposes it was collected.
- Compliance with legal and regulatory framework is achieved, monitored and maintained.
- Risk assessment is undertaken to determine appropriate, effective and affordable information governance controls are in place.
- Staff awareness with regard to their responsibilities is routinely assessed, appropriate education and awareness is provided

5.3 This policy must be read with the Information Security, IT Acceptable Use Policy, Trust Confidentiality and Multimedia Policies.

6. Roles and Responsibilities

6.1. Chief Executive

Owner of the Trust infrastructure security and responsible for signing off the Trusts compliance with NHG IT Security standards

6.2 Director of Human Resources and Organisational Development

Responsible for authorising and overseeing any investigation and disciplinary proceedings relating to the use of misuse of Trust system.

6.3. Chief Information Officer (SIRO)

The Chief Information Officer is the Senior Information Risk Owner (SIRO). The SIRO is responsible for the IT Infrastructure supporting the provision of trust network and business systems. The SIRO is strategically and operationally responsible for enterprise-wide IT security and is nominated with the responsibility for the identification and management of risks to information held on Trust systems (paper or electronic) and accountable for those risks to the Trust.

6.4. Information Security Committee

Responsible for all aspects of information and technology security including:

- the technical security of the infrastructure,
- identifying possible threats relating to information security,
- the security of IT systems and processes including access control and audit,
- ensuring that the holding, processing, sharing and transfer of data meets the strict requirements of the Data Security and Protection Toolkit and complies with the Confidentiality Policy overseen by the Caldicott Committee,
- Publicising the Acceptable Use Policy.

6.5. Heads of Information Governance and IT Operational Services supported by the Deputy Information Governance Lead

Act as the Trust’s IT Security Operational Team and are responsible for:

- Leading on IT security breaches investigations

- Monitoring and reporting actual or potential IT security breaches to the SIRO, Caldicott Guardian and Trust Executive team
- Ensuring security incidents are followed-up as appropriate,
- Ensuring compliance with the policy is monitored as required.

6.6. Service Directors

Responsible for ensuring staff awareness and adherence to this Policy.

6.7 Senior Managers

- Ensuring their staff are aware of this policy and understand their responsibilities,
- Identifying and providing secure access to equipment that their staff may use to access trust network and systems
- Monitor that their staff are following this policy.

6.8. All Trust Staff

- Responsible for complying with the Policy whenever they access / use / share / archive information on the trust network and systems
- must keep their network account passphrase secure,
- must only use their own login to access the network
- must report any breaches of this policy **immediately**
- must undertake annual information governance training

6.9. Digital Services

- Provide NHS Digital compliant, secure and cost-effective means of access to the information employees need to undertake their work,
- monitor employees network activities,
- effectively manage and authorise the appropriate connection and use of the system,
- regularly review the security effectiveness of access to information.

7. Compliance with IG Standards (Including GDPR)

It is required that SLAM and all organisations with access to NHS patient data and system must use Data Security and Protection Toolkit (DSP Toolkit) to provide assurance that they are committed to good data security and personal data is handled correctly. For SLAM to fully comply with IG standards, it must submit a satisfactory toolkit. A satisfactory toolkit demonstrates compliance with Data Protection Act 2018, GDPR and other legislation that underpins Information Governance.

7.1 Data Security and Protection Toolkit (DSP Toolkit)

The Data Security and Protection Toolkit was introduced in April 2018, it replaced the previous Information Governance toolkit. The Data Security and Protection Toolkit is an online self-assessment tool that enables SLAM to measure and publish their performance against the National Data Guardian's ten data security standards.

7.1.1 As part of demonstrating compliance the Trust must have policies covering Data Protection Act 2018, Confidentiality, Data Quality, Records Management, Data Security, Registration Authority and Network Security.

7.2 Staff Responsibilities under Each Standard

Data Security Standard 1

Staff must 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.

Staff responsibilities

Staff must familiarise themselves with IG policies listed in **section 6** of this policy

- Read the Trust's Privacy notice. The Privacy document covers what information slam collects, how it is used, and the legal basis for the use of information, where it is stored and rights of all stakeholders relating to the use of their information. The privacy notice can be found at https://www.slam.nhs.uk/about-us/privacy-and-gdpr. All staff should take an active step to sign post service users to the notice should they wish to know their rights on how SLAM processes their data.

- All grouped records of processing activities are documented and recorded as an Information Asset (***Section 7 of the policy provides details of information asset)***

- **Data Protection Impact Assessment (DPIA).** All staff must ensure a review of their processing activities to ensure that they are operating in compliance with the DPA 2018 and GDPR. This is done via completing a DPIA. ***Section 7 of the policy covers how and when completing a DPIA is required.*** Completed DPIAs are available from the Information Governance Office.

Data Security Standard 2

Standard details*:* 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

Staff responsibilities

- ➢ All new starters must attend the Data Security session covered on the Trust Values day induction or other programmes for new starters relating to IG across the Trust.

- ➢ Staff should endeavour to participate in completing Information Governance surveys. Completing the survey helps the information governance team identify training needs for IG across the Trust.

Data Security Standard 3

Standard details: All staff must complete appropriate annual data security training and pass a mandatory test.

Staff responsibilities

- ➢ All staff must complete their annual Data Security (Information Governance) training annually. Section of this policy covers type of training staff might need to take depending on their job role.

Data Security Standard 4

Standard details: 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.

Staff responsibilities

- All managers in the Trust must notify Digital Services when a staff member leaves the organisation.
- Staff should always ensure contact details on the address book are kept up-to-date.
- Staff must be aware of IT Acceptable usage banner displayed when logging into system, and note their personal accountability.

Data Security Standard 5

Standard details: 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. Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes.

Staff responsibilities

- All data and information related Incidents must be reported as soon as reasonably possible.
- Staff should contact the Information Governance team immediately on all serious incident or in an event of any data loss
- All services and departments must endeavour to work with the IG team to mitigate risks after incidents occur.

Data Security Standard 6

Standard details: Cyber-attacks against services are identified, 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.

Staff responsibilities

- All users of SLaM email MUST be mindful of suspicious emails and online scams designed to capture your personal details, such as passwords, financial information. Follow alerts and guidance from SLaM Digital Services and report incidents related to cyber security

- Staff must read Information Security Policy, IT Acceptable Use Policies and data security / IG awareness materials posted on Yammer and Trust Intranet.

- It is responsibility of staff to maintain their knowledge and undertake annual refresher training on data security and IG

Data Security Standard 7
Standard details: 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
Staff responsibilities ➢ Staff should support business continuity plans (BCP) across the trust and familiarise themselves with local emergency planning procedures. ➢ Senior staff in the Trust with operational responsibilities must have in place practicable, and up-to-date BCPs for their services that link with Digital Services BCP

Data Security Standard 8
Standard details: No unsupported operating systems, software or internet browsers are used within the IT estate. - ***This standard predominantly sits with the Digital Services technical team***

Data Security Standard 9
Standard details: 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. - ***This standard predominantly sits with the Digital Services technical team***

Data Security Standard 10
Standard details: suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
Staff responsibilities ➢ Contracts with all third parties that handle personal information must be compliant with GDPR and the Data Protection Act 2018 ➢ Staff must ensure they undertake basic due diligence against each supplier according to data protection legislation. This often requires a risk assessment called Data Protection Impact Assessment (DPIA – see section 9).

8. Policies under IG Framework

8.1 Trust Confidentiality Policy

Sensitive personal confidential data must be kept confidential in accordance with the Caldicott principles and the regulations outlined in the Data Protection Act(1998), DPA18, GDPR and Common Law Duty of confidentiality.

8.1.1 The Trust's legal obligations for data protection, information sharing, disclosures, subject access and service user rights to confidentiality are outlined in the Confidentiality Policy.

It outlines the standards for the sharing of clinical information with other health organisations and agencies in a controlled manner.

8.1.2 Sharing must be consistent with the interests of the service user. In some circumstances, the public interest must be taken into account by referring to relevant legislation such as Health and Social Care Act 2012, Crime and Disorder Act 1998, Children Act 1989.

8.2 **Information Sharing Framework for South East London** provides the standards for a uniform approach to information sharing with all partner agencies.

8.2.1 The framework ensures compliance with the DPA18, GDPR, Access to Health Records Act (1990), Human Rights Act (1998) and common law of confidentiality.

8.2.2 The Trust Confidentiality Policy, procedures and compliance are reviewed via the Information Governance Toolkit annual self-assessment. A separate Human Resources Data Protection Policy is available for the protection of personal confidential staff information.

8.3 ***Clinical Records Policy*** governs the management, handling and retention of clinical records. This policy covers the full clinical information cycle, including the purpose of these records, clinical records keeping standards, retention and preservation schedules with links to the Confidentiality Policy for guidance on access to records.

8.3.1 The Clinical Systems Implementation and Support Manager Leads annual review to ensure compliance with best practice standards of record keeping and records management with all clinical teams in accordance with the NHS Litigation Authority (NHSLA) Standards. The action plan arising from this review is reviewed regularly by the Caldicott Committee.

8.3.2 The former policy on copying letters to patients has been replaced by the Information Governance Policy under section 13

8.4 ***Multimedia Policy*** outlines the guidelines to ensure multimedia (audio-visual) records created during the course of clinical care, research and training are generated with the consent of the individuals involved, used and stored in accordance with relevant national guidelines and disposed of appropriately once the purpose of creation has been served. The policy also outlines instance where service users wish to record their health and social care consultation.

8.5 **Corporate Records Policy** defines the structure for the Trust to ensure adequate maintenance of corporate records and their effective management and control at best value, commensurate with legal, operational and information requirements. The corporate records standards in this policy relate to all corporate records, which are defined as information created or received in the course of business and captured in a readable form in any medium, providing evidence of the functions, activities and transactions. They include administrative records (including human resources, estates, financial and accounting records, contract records, litigation and records associated with complaint-handling) in all formats including paper, electronic, e-mail, microfilm, film and relevant images

8.6 **Information Security Policy:** All users of SLAM Digital Services SHOULD make every effort to use digital and online resources appropriately and consider using them rather than creating paper copies. Users should avoid paperwork duplication. Don’t print emails, ePJS records unless absolutely necessary. Printed copies are easily lost. Users MUST use secure mobile devices, such as trust provided tablets, smartphones instead.

8.6.1 Users MUST dispose of all information securely. If you have to print, you MUST shred securely as soon as the print-out has been used. If shredding is not possible, all MUST ensure to dispose of confidential personal information and sensitive corporate information in confidential waste bags provided. These confidential bags must be stored away from public areas and must be collected for secure off-site destruction in a timely manner.

8.6.2 Security arrangements in your work place are crucial. All MUST follow the building and site security rules at work and do not allow unauthorised people unvetted access to areas that are not for public use.

8.7 IT Acceptable Use Policy: It is the responsibility of all users to ensure that they adhere to the instructions laid down in the Acceptable Use Policy. Before a new user can be allocated a trust network account, they must understand and agree to the terms of this policy.

8.7.1 The instructions contained in the policy are special restrictions in force with regard to the Trust controlled and processed information and, are clarifications or additions to the normal security measures in force within the Trust.

8.7.2 All usual security precautions must be taken in addition to these specific requirements.

There are also strict NHS security requirements for Trust networks that are connected to the national NHS network by way of mandated compliance with the Data Security and Protection Toolkit.

9. Data Protection Impact Assessment (DPIA)

9.1 The Data Protection Impact Assessment (DPIA) is a tool which helps assess data protection and privacy risks to individuals in the collection, use and disclosure of information.

9.2 The core principles of conducting a DPIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals, the protection of their personal data and can be used for a number of situations such as:

- A new IT system for storing and accessing personal data. This could be a spreadsheet, simple database or full scale clinical system.

- A proposal to identify people in a particular group or demographic and initiate a course of action, for example a mail shot.

- Using existing data for a new and unexpected (by the data subject) or more intrusive purpose.

- A new surveillance system (especially one which monitors members of the public or patients) for example Wi-Fi tracking or tagging

- A new database which consolidates information held by separate parts of the organisation.

- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

- A data sharing initiative/agreement where two or more organisations seek to share, pool or link sets of personal data.

9.3 A project which has included a DPIA at the very start of the project, and updated as the project progresses, should result in the project being less privacy intrusive and therefore less likely to affect individuals in a negative way. The reasons to undertake a DPIA include:

- To identify privacy risks to individuals;
- To identify privacy, data protection and General Data Protection Regulation (GDPR) compliance liabilities for your organisation;
- To instil public trust and confidence in your project, process, tool, service, policy etc.;
- To inform your communications strategy (how you will inform your service users, citizens);
- To support public transparency as DPIAs are disclosable under the Freedom of Information Act;
- To avoid expensive, inadequate "bolt- on" solutions;
- To protect the reputation of the organisation;
- To reduce the likelihood of regulatory action against the organisation.

9.3.1 The trust has a library of all conducted DPIAs which are available upon request from informationgovernance@slam.nhs.uk

10. Information Governance Training

10.1 Information Governance Training is mandatory to all staff with a requirement to undertake annual refreshers. All Trust staff **must** attend the compulsory information governance training as part of their induction at the start of their employment with the Trust and refresh at annual intervals.

10.2 In addition to classroom training, the Trust provides an e-learning alternative on LEAP system.

10.3 The IG department can also provide bespoke training. All training requests and queries must be made to the informationgovernance@slam.nhs.uk.

11. Information Asset Register

11.1 As part the Trust's compliance with DPA18, we are required to capture all incoming and outgoing personal data, special category data (sensitive data) and business related data. All the captured data flows will be groups into Borough/Operational Directorates and registered as Information Asset (IA).

11.2 The Information Governance (IG) team will be responsible for coordinating this exercise. The Trust is required to provide evidence of this activity to NHS Digital, CQC and Information Commissioners Office (regulators).

11.3 The information asset register (IAR) is vital to the centralised management and oversight of performance against new legal requirements and standards. It has been designed to provide both assurance and evidence against new data security standards, especially those processing personal confidential data.

11.4 The IG team is providing training and guidance to all nominated information asset owners (IAO) and information asset administrators (IAA) to support the delivery of the required assurance and evidence.

11.5 It is recommended that all services nominate an IAO and IAA. All information assets must be reviewed every 12 months with all the data flows approved by the Board or equivalent committee. The IG team will work with all IAO and IAA when required.

11.6 The Trust overall Information asset register will then be approved by the Information Security Committee with a report going to the Trust board.

12. Legal Requirement

12.1 Trust provided internet and Digital Service equipment must not be used to violate the laws and regulations of the United Kingdom. Use of the Trust's resources for any illegal activity constitutes disciplinary matter. Any illegal activity will be reported to the appropriate authority for future investigation.

13. Correspondence with Patients

13.1 All clinical services are expected to engage and involve service users in their own care. Additionally, services need to be transparent with service users about their treatment and care. It is also service users' data subject right to have access to their health information. In the NHS Long Term Plan, it is a key objective of all NHS organisations to provide service users online access to their health information.

13.2 In order to achieve these objectives, all clinical services are required to check service users' communication preferences. The trust encourages use of secure SLaM NHS email to communicate with service users. Staff and service users must be mindful of data security threats while using email. Even secure email systems such as SLaM NHS email, user errors may lead to misdirection of email and result in data breaches. All staff much make sure they undertake annual IG training and stay aware of data security guidance from SLaM Digital Services.

13.3 Clinical care co-ordinators should check service users' preferences to ensure:

i. Whether they would like to provide their email address to receive correspondence and copies of letters electronically,

ii. Whether they would like to provide a mobile phone number to receive calls and text messages

iii. Indicate their preferred mode of communications (e.g. post, email, phone)

13.4 Clinical care co-ordinators should make sure this information is recorded on ePJS under "managing patient information" section. Staff are strongly advised to check regularly for updates on contact details. It is recommended to remind service users of their preferences to ensure they have a fair chance to review and update them when required.

14. Monitoring Compliance

What will be monitored i.e. measurable policy objective	Method of Monitoring	Monitoring frequency	Position responsible for performing the monitoring/ performing co-ordinating	Group(s)/committee (s) monitoring is reported to, inc responsibility for action plans and changes in practice as a result
Information Governance compliance	NHS Digital Data Security and Protection Toolkit and Internal Audit Independent IG Review	Annual (with frequent updates)	Head of Information Governance and Deputy IG Lead	Caldicott , Information Security and FOI Committees
Confidentiality, information sharing, Data Protection Act (2018),	IG Assurance Programme	Annual	Head of Information Governance	Caldicott Committee (and Information Security Committee for technical aspects)
Confidentiality, information sharing, Data Protection Act (2018) incidents	Data breach incident reports and quarterly lesson learned report	Quarterly	Head of Information Governance	Caldicott Committee (and Information Security Committee for technical incidents)
Health records management and data quality	Health Records Review	Annual	Clinical Systems Manager	Caldicott Committee
Corporate Records Management	Corporate Records Review	Annual	Head of Information Governance and the Trust Secretary	Freedom of Information Committee
Data Quality	Health Intelligence and Performance Management	Monthly	Head of Performance and Head of BI	Intelligent Information Group

15. Associated Documentation

- Acceptable Use Policy
- Records Management Code of Practice for Health and Social Care 2016.
- Confidentiality Policy
- Information Risk, Incident and Forensic Readiness Policy
- Information Security Policy

16. Freedom of Information Act 2000

6.1 All Trust policies are public documents. They will be listed on the Trusts FOI document schedule and may be requested by any member of the public under the Freedom of Information Act (2000).

Appendix 1

PART 1: Equality relevance checklist

The following questions can help you to determine whether the policy, function or service development is relevant to equality, discrimination or good relations:

- Does it affect service users, employees or the wider community? Note: relevance depends not just on the number of those affected but on the significance of the impact on them.
- Is it likely to affect people with any of the protected characteristics (see below) differently?
- Is it a major change significantly affecting how functions are delivered?
- Will it have a significant impact on how the organisation operates in terms of equality, discrimination or good relations?
- Does it relate to functions that are important to people with particular protected characteristics or to an area with known inequalities, discrimination or prejudice?

Name of the policy or service development:								
Is the policy or service development relevant to equality, discrimination or good relations for people with protected characteristics below? **Please select yes or no for each protected characteristic below**								
Age	**Disability**	**Gender re-assignment**	**Pregnancy & Maternity**	**Race**	**Religion and Belief**	**Sex**	**Sexual Orientation**	**Marriage & Civil Partnership** *(Only if considering employment issues)*
No	Yes	Yes	No	No	No	No	No	No
If yes to any, please complete Part 2: Equality Impact Assessment **If not relevant to any please state why:**								

Date completed: 12/08/2019
Name of person completing: Claire Delaney-Pope
Operational Directorate/Borough: Corporate
Service / Department: Information Governance / Digital Services

Please send an electronic copy of the completed EIA relevance checklist to:

1. macius.kurowski@slam.nhs.uk
2. Your Operational Directorate/Borough Equality Lead

PART 2: Equality Impact Assessment

1. Name of policy or service development being assessed?
Information Governance Policy

2. Name of lead person responsible for the policy or service development?
Claire Delaney-Pope, Deputy IG Lead

3. Describe the policy or service development
What are its objectives and intended outcomes?
Objectives:
Intended Outcomes:

- To ensure that controls are in place to protect the Trust IT Estate and all information assets.
- To ensure the protection of personal identifiable information both within the boundaries of the Trust and during inbound and outbound transfer.
- To ensure that users of IT Services are aware of the regulations, standards and procedures required in providing a secure IT Service.
- To ensure the Trust works in accordance with the principles of the Data Protection Act (2018)
- To ensure all information-processing systems must be protected to minimise the risk of adverse events such as accidents, negligence and malicious damage which could jeopardise business intelligence activity, care delivery and the legal rights of both clients and staff of the Trust.

What is the timetable for its development and implementation? The policy was consulted with Digital Services management team and the Information Security Committee. To be immediately available for all Trust staff.

4. What evidence have you considered to understand the impact of the policy or service development on people with different protected characteristics
This is a revised policy that has been updated to keep it in line with national standards and the data protection legislation. The policy was consulted Digital Services management team and the Information Security Committee.

5. Have you explained, consulted or involved people who might be affected by the policy or service development?
N/A

6. Does the evidence you have considered suggest that the policy or service development could have a potentially positive or negative impact on equality, discrimination or good relations for people with protected characteristics?
(Please select yes or no for each relevant protected characteristic below)

Age	**Positive impact:** Yes	**Negative impact:** no

Please summarise potential impacts:
It is anticipated the Information Governance policy will have a positive impact as it details data subject rights and the various support for individuals to access their data, The policy

ensures that there are various ways to access information that isn't just electronic communication thus potentially positively impacting those of all ages.		
Disability	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated this policy will have a positive impact as it highlights the rights of the data subject which includes the various means to request and access personal data. This is in a variety of ways which will support those with disabilities.		
Gender re-assignment	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the policy will have a positive impact as it outlines how to collect and protect data from patients who are undertaken or have undertook gender re-assignment. This is also further documented in the Clinical Records policy		
Race	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: The policy will demonstrate the rights of all data subjects and will ensure demographic data is collected and stored appropriately.		
Pregnancy & Maternity	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: The policy will demonstrate the rights of all data subjects		
Religion and Belief	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: The policy will demonstrate the rights of all data subjects and emphasises how special character data is collected and stored.		
Sex	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: The policy will demonstrate the rights of all data subjects		
Sexual Orientation	**Positive impact:** Yes	**Negative impact:** No
The policy will demonstrate the rights of all data subjects and emphasises how special character data is collected under GDPR.		
Marriage & Civil Partnership *(Only if considering employment issues)*	**Positive impact:** No	**Negative impact:** No
Please summarise potential impacts:		
Other (e.g. Carers)	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Information Governance policy will have a positive impact on service users by ensuring information is protected from data security threats through the improved way of collecting data under GDPR. It also highlights the data subject rights and how to access records The policy also enforces the secure destruction of confidential information.		

7. Are there changes or practical measures that you can take to mitigate negative impacts or maximise positive impacts you have identified?

N/A

8. What process has been established to review the effects of the policy or service development on equality, discrimination and good relations once it is implemented?

N/A

PART 3: Equality Impact Assessment Action plan

Potential impact	Proposed actions	Responsible/ lead person	Timescale	Progress
Review actual equality impacts of policy	Review policy EIA	Policy Lead	May 2020	

Date completed: 12/08/2019
Name of person completing: ***Claire Delaney-Pope***
Borough/Operational Directorate: ***Corporate***
Service / Department: ***Digital Service***

Appendix 2

Human Rights Act Impact Assessment

To be completed and attached to any procedural document when submitted to an appropriate committee for consideration and approval. If any potential infringements of Human Rights are identified, i.e. by answering Yes to any of the sections below, note them in the Comments box and then refer the documents to SLaM Legal Services for further review.

For advice in completing the Assessment please contact Tony Konzon, Claims and Litigation Manager (Anthony.Konzon@slam.nhs.uk)

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
The Human Rights Act allows for the following relevant rights listed below. Does the policy/guidance NEGATIVELY affect any of these rights?		
Article 2 - Right to Life [Resuscitation /experimental treatments, care of at risk patients]	No	
Article 3 - Freedom from torture, inhumane or degrading treatment or punishment [physical & mental wellbeing - potentially this could apply to some forms of treatment or patient management]	No	
Article 5 – Right to Liberty and security of persons i.e. freedom from detention unless justified in law e.g. detained under the Mental Health Act [Safeguarding issues]	No	
Article 6 – Right to a Fair Trial, public hearing before an independent and impartial tribunal within a reasonable time [complaints/grievances]	No	
Article 8 – Respect for Private and Family Life, home and correspondence / all other communications [right to choose, right to bodily integrity i.e. consent to treatment, Restrictions on visitors, Disclosure issues]	No	
Article 9 - Freedom of thought, conscience and religion [Religious and language issues]	No	
Article 10 - Freedom of expression and to receive and impart information and ideas without interference. [withholding information]	No	
Article 11 - Freedom of assembly and association	No	

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
Article 14 - Freedom from all discrimination	No	

Name of person completing the Initial HRA Assessment:	Deputy IG Lead
Date:	11/03/2019
Person in Legal Services completing the further HRA Assessment (if required):	
Date:	