Barnet, Enfield and Haringey NHS
Mental Health NHS Trust

A University Teaching Trust

Information Governance Policy

Version:	5.0
Policy Number:	16931
Policy Lead/Author & position:	Mary Olubi IG Manager / Data Protection Officer
Ward / Department:	Corporate
Approving Committee / Group:	Information Governance Group
Ratified by:	Policy Development &Review Group
Date Approved/Ratified:	March 2011
Previous Reviewed Dates:	June 2014, June 2017
Date of Next Review:	June 2023
Relevant NHSLA Standard(s):	Nil
Target Audience	All Trust employees

EQUALITY STATEMENT

Barnet, Enfield and Haringey NHS 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. It takes into account its legal obligations under Equality Act 2010, the Human Rights Act 1998 and other relevant legislation.

This document has been assessed to ensure that no one affected will receive less favourable treatment on the basis of a protected characteristic - age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) and sexual orientation.

The Trust embraces the four staff pledges in the NHS Constitution and this policy is consistent with these pledges. The Trust is also committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff and volunteers to share this commitment.

The Trust will make accessible versions of this document available if requested by members of the public, service users or staff who have particular communications needs.

This Policy supports the BEHMHT Vision and Values:

Trust Vision

To support healthy lives and healthy communities through the provision of excellent integrated mental and community healthcare.

Trust Values

• Compassion.

• Respect

• Working Together

• Being Positive

Table of Contents

Document History

CONSULTATION RECORD OF PROCEDURAL DOCUMENT FORM

Name and Title of Individual	Date Consulted
Sarah Wilkins Chief Information and Performance Manager (Senior Information Risk Officer – SIRO)	October 2020
Contributing Authors: Chief Clinical Information Officer	November 2020
Name of Committee	**Date of Committee**
Information Governance Group (IGG)	3 November 2020

Version Control Summary

Version	Date	Section	Author	Comments
1.0	01/11/11	All sections	IG Manager	
1.1	09/06/14	Various sections	IG Manager	Changes to accountability, added reference to overseas transfers. Altered reference to Connecting for Health to HSCIC.
2.0	28/06/17	Various sections	IG Lead	Changes made in accordance with new guidance pending implementation of General Data Protection Regulations due for implementation May 2018.
3.0	Dec 2017	Various sections		Changes made in accordance with new guidance. Information relating to consent mechanisms added.
3.1	April 2019	Section 7	DPO	Guidance relating to using portable media added
4.0	June 2020	Review of Sections	IG Manager / DPO	Complete review of Policy

4.1	October 2020	All sections	IG Manager / DPO	Update of Policy lead name and job title. Reviewed to align with NHSE Policy template and IG guidance documents. to ensure GDPR & DPA 2018 compliance. Minor update to roles and responsibility, Head of Business changed to Deputy Chief Information Officer. IG Role Structure Chart removed (Section 12.1). Safe Haven section reworded to reflect current trust position.
4.2	January 2021	Various	IG Manager	Document update to include of IG Group review comments.
4.3	January 2021		IG Manager	Update to Trust vision and values section
5.0	18 January 2021			Final approved version.

1. Introduction

The role of Barnet, Enfield and Haringey Mental Health Trust (BEHMHT), is to provide healthcare, and best possible outcomes for patients. In doing so, BEHMHT will seek to meet the objectives prescribed in the Mandate and to uphold the NHS Constitution. This policy is important because it will help the people who work for the Trust to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

This policy sets out the intentions of BEHMHT to manage the information governance agenda within its remit to the standards required by law and regulation. Specifically, Data Protection Legislation (Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation). In doing so, supports high-quality healthcare provision, through accurate, accessible and appropriately governed information.

Information is a vital asset both in terms of clinical management of individual service users and the effective control of services and resources. Reliable information is a fundamental requirement of the NHS and crucial for:

- The ability to make informed decisions related to patient care.
- The ability to decide what services to commission for the future.
- Performance management and improvement planning

A robust Information Governance (IG) framework gives assurance that the Trust handles personal and non-personal information efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service.

The term information governance encompasses information security, staff and patient confidentiality, information sharing, records management, data quality and freedom of information.

The NHS and the administration of the NHS are dependent on the appropriate use of personal data, and the management of secondary uses of this data and business sensitive data.

2. Purpose and Aim

The purpose and aim of this policy is to ensure that information is efficiently managed and that appropriate policies, clear procedures and levels of accountability are in place to provide a robust governance framework for information management.

Information governance ensures processes, confidentiality and security controls are in place and sets standards of quality and ethical use of personal data. Corporate records must also be managed appropriately and where possible provided to the public under the appropriate legislation (Freedom of Information Act 2000 and Environmental Information Regulations 2004) to ensure transparency and accountability.

All staff are responsible to abide and contributes towards effective and responsible governance of information.

This policy aims to ensure that data is:

- Held securely and confidentially;
- Obtained fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically; and
- Shared and disclosed appropriately and lawfully.

The Trust aims for the management of information and associated risk include:

- Effective and efficient management of information for the care of service users and the management of the care service;
- Actively advance the management of information to improve the provision of services, information and care of patients;
- Engage with partner organisations and where appropriate and lawfully share information to support care and the public interest;
- Discharge its obligations to disclose information in response to lawful requests with due regard to its duties of confidence by following clear and systematic processes;
- Ensure that systems and processes are effective to ensure the confidentiality and security of personal and other sensitive information;
- Ensure that all information and data processed, held and managed is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness;
- Ensure that all information and data is held in a consistent and systematic manner that ensures its accessibility, accuracy and integrity throughout its lifecycle;
- To actively provide information in line with the Freedom of Information Act 2000 and other regulatory or organisation requirements;
- Ensure those working for and on behalf of the Trust, are informed, trained and active in the appropriate management of information; and
- To ensure that change is undertaken in a structured and systematic manner that ensures information governance issues are dealt with in a timely, proportionate and appropriate way.

This policy also sets out processes to ensure the Trust information asset is protected from threats either deliberate or accidental by ensuring the following:

- Information is protected against unauthorised access;

- Confidentiality of information will be assured;
- Integrity of information is maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information Governance training will be available to all staff; and
- All breaches of information security, actual or suspected, will be reported and investigated by the Information Governance Manager / DPO
- The Trust recognises that effective information management is fundamental to proper administration and operational effectiveness, and is an enabler to the achievement of our strategic goals.

2.1 Objectives

The Barnet, Enfield and Haringey Trust Board is committed to ensuring that:

- Information that relates to patients and staff is processed, protected and disclosed appropriately to provide improved healthcare and decisions for patients.
- Information related to its functions, activities and decisions is managed to the appropriate standards.
- The right information, in the right format, to the right people at the right time.

3. Scope

This policy applies to:

- All information and data held and processed by the Trust which must be managed and held within a controlled environment, including the personal data of patients and staff, as well as corporate information. It applies to information, regardless of format, and includes legacy data held by the organisation.
- All permanent, contract or temporary staff of the Trust and any third parties who have access to the Trust premises, systems or information. Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual or voluntary basis;
- Information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed outputs from these systems, and

- All means of communicating information, both within and outside the Trust in both paper and electronic format, including data and voice transmissions, emails, post, voice and video conferencing.

The Trust believes that its internal management processes will be improved by the greater availability of information that will grow by the recognition of information governance as a designated corporate function.

4. The use of Information

All information must be created, used and managed in a professional manner, as described in the Information Management Policy. It must be accessible to the organisation on a long-term basis and must be stored in a systematic and consistent manner.

Access to information systems, such as the email, the internet or network, and records of the organisation are provided to staff for business purposes and remain the property of the Trust. All access to, and use must be appropriate and in line with the discharge of their duties.

As staffs create information, they are doing so on behalf of the organisation, for example when sending emails, and are accountable for the information they create, for its appropriateness and accessibility.

4.1 Use of Personal Data

Personal data can relate to information about patients, service users and members of staff that describes an identifiable person. It does not have to include particular demographic information, such as name and address but can consist of a combination of factors that would make it possible to identify the person. Information is provided to the NHS, with the expectation of confidentiality in a healthcare setting.

Personal data is also subject to a duty of confidentiality, because it relates to a patient; we refer to this as personal confidential data. It is important for staff and best working practice to account for this and to ensure that any secondary use of personal confidential data, for non-care (Direct Care) purposes, is done in accordance with legal and organisational requirements.

The Trust has a Privacy Notice published on it's website, which details what personal data is held and processed, for what purpose it is used, who it is shared with, and what governs that process. Each service within the Trust must provide a clear statement for their area of responsibility.

4.2 Use of Information to improve performance

The Trust will actively seek opportunities to improve its performance across its customer base by the better use of information and data. These include:

- Use of anonymised or de-identified patient data to inform better health care decisions for individuals and the community;

- To review processes and functions within the organisation to ensure efficient and effective data processing; and

- To engage with partner organisations to identify appropriate information sharing which ensures that the patient and public can exercise choice and are kept informed.

All change processes must follow the standard required, as set out in the Change Management Policy, including Data Protection Impact Assessment (DPIA). All staff managing change must ensure that they identify any potential information governance requirements and risk when scoping the business case for any change.

5. Data Quality and Records Management

The Data Quality and Records Management policies outline the standards and procedures for the effective management of records and data quality assurance in accordance with National Standards. Both policies are available on the Trust intranet.

In order to support effective care provision and commissioning to support efficiency, all systems and standard working practice involved in the processing of information, must ensure the accuracy and quality of information.

Data quality as per in the Information Quality Policy requires:

- **Accessibility** – information can be accessed quickly and efficiently through the use of systematic and constituent filing.
- **Accuracy** – information is accurate, with systems that support this work through guidance.
- **Completeness** – the relevant information required is identified and working practice ensures it is routinely captured.
- **Relevance** – information is kept relevant to the issues rather than for convenience with appropriate management and structure.
- **Timeliness** – information is recorded as close to possible to when being gathered and can be accessed quickly and efficiently.

6. Disclosure and Sharing Information

As a public body, the Trust can only share personal confidential data when it is legally permissible.

This includes:

- The common law duty of confidence, which extends after death.
- Data protection legislation.

Any basis of disclosure and sharing needs to be understood and clearly stated before it is undertaken. This decision must demonstrate that the disclosure or sharing:

- Is reasonable and done in good faith for a clear intention;

- Lawful and relevant to the purpose intended;
- With grounds that are in the public interest.

Data sharing in the NHS is also governed by the Caldicott Principles which supports the legal framework.

Disclosure or sharing of personal confidential data requires one of the following conditions to be met:

- The informed and valid consent of the individual, balanced against any duty of care and consideration of capability to provide that consent;
- Disclosure is in the public interest, which must demonstrate consideration of the balance of public interest against the individual and provision of a confidential service; or
- Disclosure is in accordance with the law.

All routine sharing of information must be supported by clear statement and clauses in a Data Sharing Agreement (DSA) that can be made available to the public or patients. This Privacy notice must detail the type of information being shared, who is it is being shared with and to what purpose and benefit. In addition, all routine information sharing must be accompanied by a current data sharing agreement or legally binding agreement that sets out the all relevant issues, undertakings and processes for the sharing.

6.1 Public rights of disclosure

All staff are reminded that there are several pieces of legislation that require information to be released to the public, the Freedom of Information Act 2000, Environmental Information Regulations 2004), General Data Protection Regulation (GDPR) and Data Protection 2018 , under the Subject Access Request (for living Persons), or Access to Health Records Act 1990 for those with a claim to the estate of the deceased.

6.2 Freedom of Information Act 2000 and Environmental Information Regulations 2004

2004 is a law giving people the general right to see recorded information held by public authorities. The Act helps people get a better understanding of how public authorities carry out their duties, make decisions and spend public money.

All staff are accountable under the FOI Act and compliance with the Act is a legal requirement. The Trust has a Freedom of Information Policy and Protocol which is available on the internet, and illustrates the Trust's procedure for dealing with information requests under the Act".

A detail of the Trust policy on active disclosure and compliance with the Freedom of Information Act is outlined in the organisation's Freedom of Information Policy and associated protocols and procedures.

7. Transferring of information

All transfers of information within and outside the Trust must be managed, comply with the information security requirements and follow clear process. All teams must have a clear statement of their inward and outward flows of personal data and personal confidential data in the form of an Asset and Data Flow Mapping Register. This must be maintained and regularly reviewed and updated.

The Asset and Data Flow Mapping Register must identify:

- The appropriate method, and inherent risks, of the transfer;
- The contact point and details to which the information is routinely transferred. All contact points should identify a team and position, rather than an individual to which the information is being transferred; and
- How the transfer is confirmed and completed.

In addition, where the transfer of information involves personal or identifiable data:

- The category of data subject, purpose and legal justification for transferring the information
- Security standards of the method of transfer.

It is expected that most transfers of information will be routine and follow an identified process.

The transfers of information within the Trust and between external organisations must be managed in an appropriate manner and by secure methods with any risks identified and managed.

8 Safe Havens

Safe Havens is no longer in place because the Trust no longer use fax machines.

9. Information Security

The purpose of information security is to ensure business continuity in order to minimise the impact of security-related incidents and to ensure the integrity of the information and data processed by the Trust, as described in the Information Security Policy.

Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to security.

Information security is both the technical and physical. It ranges from the security of networks, to the use of appropriate passwords by staff and storage of confidential information in secure environments.

All staff contributes towards the security of information and Information Asset Owners are required to have a clear statement on the information security and risks in place for the assets within their remit.

Information security has four basic components:

- **Confidentiality**: assuring that sensitive information or data is accessible to only authorised individuals and is not disclosed to unauthorised individuals or the public.
- **Integrity**: safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.

- **Availability**: ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

- **Accountability** – Users are held responsible for their use of information.

9.1 Mobile devices

Trust provided mobile and portable devices must be used at all times, because they are encrypted and built with standard protection software.

The use of USBs will be discouraged to protect confidential data but the Trust will acknowledge that there may be times when staffs need to transfer information this way. This will be permitted where encrypted devices are used only to ensure the protection of the data. Staff should seek advice from the IM&T where they are unsure to ensure there device meets the expected NHS standard.

Further information is detailed in the Trust Information Security Policy.

10. Monitoring and compliance

This policy and the associated controls: policies, protocols and procedures will be monitored through the risk management process for the Trust. The information governance risk register will be reviewed on a regular basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the risks and information flows associated with the information assets utilised to fulfil the business functions and activities within their remit.

11. Non-Compliance

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible.
Failure to maintain these standards can result in criminal proceedings against the individual.

12. Review

Review will take place three years or earlier (annually) until rescinded or superseded, due to legal or national policy changes.

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available in the policy register for the organisation. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

13. Implementation and dissemination

The updated policy, once approved by the Information Governance Group, will be shared with all staff through staff briefing to support this dissemination and updated on the intranet.

Awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis.

14. Roles and Responsibilities

A number of key roles and committees will support the duties established in this Policy:

The Chief Executive, as the Accountable Officer, will have overall strategic responsibility for the information governance agenda at the Trust. The Board will be responsible for ensuring that the information governance function is addressed at the strategic level and policies, procedures and related documents are approved and implemented.

The Executive Team will ensure that information governance at an operational level is accountable to the Board. The Executive Team will ensure there is an adequate level of resources, funding and expertise to deal with the range of issues that arise across the information governance function.

The Senior Information Risk Owner (SIRO), which is the Chief Performance and Information Officer, will have overall responsibility for managing information risk across the Trust and will ensure all IG and IT Security Risk Registers are maintained and reviewed periodically. This will include ensuring the Board is notified of any high risk processing activities for Board approval when necessary. The SIRO is also strategically responsible for the record and document management processes of the Trust.

The Trust's Caldicott Guardian, which is the Trust's Medical Director, will have overall responsibility for ensuring all confidential information relating to patients and service users is protected and handled with appropriate safeguards.

The Trust's Data Protection Officer (DPO), who is also the **Information Governance Manager** is accountable to the Chief Information Officer will have the day-to-day operational responsibility for all aspects of information governance. The DPO will co-ordinate and mandate the Information Asset Register and oversee all ICO enquires, statutory notices and serious incidents

The Deputy Chief Information Officer also the Deputy SIRO is responsible for the network and information communication systems across the Trust and will work with the SIRO to ensure that information risk is managed appropriately. This will ensure that appropriate controls are implemented to protect sensitive information from being unauthorised and ensuring information is not passed over public networks, including the

internet.

The Trust's FOI Manager will be the contact point for all Freedom of Information and Environmental Information Requests and will co-ordinate all responses with the Trusts nominated representatives in each service area. The FOI Manager will oversee the Trust's Publication Scheme and will ensure the Trust complies with current information legislation.

The Trust's Medical Records Manager will be the contact point for all subject access requests and will co-ordinate all responses with the nominated service leads whilst also assisting with all ICO enquiries.

The Information Asset Owners of each service area who will be the Heads of Service will ensure they maintain an information asset register of the information they hold, how it is stored and who has access to it. The IAOs will understand, address and manage the risks of their assets and will ensure they have resilient and robust business continuity and back up recovery processes in place for their systems where information needs to be protected and where network dependencies and other issues exist.

All Line Managers, who will be the Information Asset Administrators (IAAs) of the information asset, will ensure that they take responsibility for controls of this IG Policy being implemented and carry out the administration requirements that are assigned to them in accordance with this Policy either via the IAO or the Data Protection Officer.

All staff will ensure will ensure they adhere to this policy and ensure all work programmes comply with the obligations and responsibilities outlined in this information governance framework. Failure to comply with this Policy may result in disciplinary action.

15. Data Security Protection Toolkit (DSPT)

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use the DSPT to provide assurance that they are practicing good data security and that personal information is handled correctly.

The DSPT is an annual assessment. As data security standards evolve, the requirements of the Toolkit are reviewed and updated to ensure they are aligned with current best practice. Organisations with access to NHS patient data must therefore review and submit their DSPT assessment in each financial year before the 31st March deadline.

The DSPT also provides organisations with a means of reporting security incidents and data breaches.

The DSP toolkit can be accessed via the following link:
https://www.dsptoolkit.nhs.uk/OrganisationSearch/RRP

16. Lead Director

The Lead Director is the Chief Information Officer

17. Associated Trust Documents:

Information Sharing Policy
Information Security Policy
Data Quality Policy
Information Governance Strategy
Information Risk Policy
Records Management Policy
Registration Authority Policy
Pseudonymisation and Annonymisation policy
Freedom of Information policy

All the above policies and documents are available on the intranet
http://staff.beh-mht.nhs.uk/

18. References

This policy has been prepared in reference to the documents listed below and should be read in conjunction with them, most are available on the Trust intranet http://staff.beh-mht.nhs.uk/

- Data Protection Legislation and Caldicott principals
- Department of Health Confidentiality NHS Code of Practice
- Department of Health Information Security Management Code of Practice
- Freedom of Information Act 2000
- Information Governance Toolkit
- Caldicott review – to share of not to share
- Information Governance Incident management

The current review is in accordance with NHS England Information Governance Policy guidance document template. https://www.england.nhs.uk/publication/information-governance-policy/

19. MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF PROCEDURAL DOCUMENTS

1.	How will the document be monitored? (please circle as appropriate)	Audit		Review ✓	Other, please specify;
		Methodology:			
2.	What is the process for reviewing results of monitoring?				
3	Report to:				
4.	Who is responsible for conducting the monitoring? (please circle as appropriate)	Information Governance Group ✓		Individual	
		Name / Title (also include position of individuals):			
5.	How often will the document be monitored? (please circle as appropriate)				Other, please specify; Every 3 years in accordance with Trust policy or changes in National legislation
		Comments:			
6	Responsibility for action planning after review				

20. EQUALITY IMPACT ASSESSMENT AND ANALYSIS FORM

This policy is produced in accordance with NHS England, Information Governance Policy Guidance.
https://www.england.nhs.uk/publication/information-governance-policy/

This policy is in accordance with NHS England document to provide guidance to all staff, on Information Governance.

21. Checklist for the Review and Approval of procedural Document

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	Title	Information Governance Policy	
	Is the title simple and clear to everyone who reads it?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	Rationale		
	Are reasons for development of the document stated?	Yes	
3.	Development Process		
	Is the method described in brief?	Yes	
	Are individuals involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	Content		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	Evidence Base		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	Approval		

	Does the document identify which committee/group will approve it?	Yes	

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	If appropriate, have the joint staff side committee (or equivalent) approved the document?	Yes	
7.	Dissemination and Implementation		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	Document Control		
	Does the document identify where it will be stored?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	Process for Monitoring Compliance		
	Are there measurable standard to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	Review Date		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	Overall Responsibility for the Document		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	