Lincolnshire Community Health Services NHS Trust

Records Management Policy

(Clinical and Corporate Records, Access to Information, Scanning Documents)

Reference No:	P_IG_28
Version:	1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Kaz Scott, Information Governance Lead
Name of responsible committee/individual:	Information Governance Management Assurance Group
Date issued:	August 2018
Review date:	August 2020
Target audience:	All staff and third party contractors employed by LCHS
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Version Control Sheet

Version	Section/Para /Appendix)	Version/Description of Amendments	Date	Author/ Amended by
1		Amalgamation of policies (P_IG_04, 11, 19, 20), content previously ratified and further content updated to reflect GDPR.	June 2018	Kaz Scott
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Contents

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Policy Statement

Background

The Trust has a duty under the Public Records Act to make arrangements for the safekeeping and eventual disposal of all types of in accordance with the schedule. This includes records controlled by organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of their format. The Act requires all public bodies to have effective systems to deliver their functions.

Records also serve the wider purposes of teaching, research and clinical audit as well as providing evidence in the event of litigation. They are also a vital source of statistical and managerial information for the day to day running and future planning of the NHS.
This policy relates to all clinical and non-clinical operational records held by the Trust and pulls together the arrangements covered by the following policies:

- Consent to Treatment Policy
- Data Protection Policy
- Safeguarding Children Policy
- Inter-Agency Information Sharing Protocol
- Risk Management Strategy
- Incident Reporting Policy
- Information Security Policy
- Information Risk Policy
- Skills for Health

Statement

The policy is split into sections and details specific procedures for achievement of the policy standards.
Staff working for the Trust will ensure that they comply with the requirements of the Data Protection (DP) Legislation, which brings together the General Data Protection Regulation (GDPR) & DP Act 2018.

Responsibilities

All staff have a responsibility for maintaining confidentiality and handling information appropriately.

Training

All staff are responsible for their own record keeping and must maintain an up to date awareness of legal and ethical issues concerning the subject.

Dissemination

The policy will be published on the Trust website.

CLINICAL AND CORPORATE RECORDS

This is the process by which the Trust manages all aspects of clinical records whether internally or externally generated and in any format or media type, from their creation to their eventual disposal.

The Trust requires records to:

- Support patient care and continuity of care;
- Support improvements in clinical effectiveness through research;
- Assist clinical and other record audits;
- Protect the interests and rights of patients and employees

All records created and maintained by the Trust are Public Records under the Public Records Act 1958 and 1967 and the Trust must ensure that Records Management policies and procedures are in accordance with the following statutory and NHS guidelines.

- Data Protection Legislation (DP)
- Freedom of Information Act 2000
- NHS Code of Practice for Confidentiality
- The Code: Professional standards of practice and behaviour for nurses and midwives
- NHSLA Risk Management Standards for NHS Trusts
- Data Security and Protection Toolkit (DSPT)

The Records Management Code of Practice for Health and Social Care 2016 has been published by the Department of Health (DH) as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

The Trust is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from doing so.

Scope and Definitions
A record is anything which contains information, electronic or paper based – in any media - which has been created or gathered as a result of the work of NHS employees, including:

- Service user healthcare/clinical records (electronic or paper based)
- Microfiche or electronically digitalised health records
- Audio and videotapes, cassettes, photographs
- Digital Records
- Computerised Records
- Emails

All staff employed within the Trust (including those on temporary contracts, students or Bank/Agency staff) who are involved in handling, contributing to or creating clinical records, making them aware of their responsibilities to meet the requirements and standards relating to the records.

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs and preserving an appropriate historical record.

The key components of records management are:

- Create, Use, Retain, Appraise, Destroy

The term **'Records Life Cycle'** describes the life of a record from its creation / receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

Accountability – adequate records are maintained to account fully and transparently for all actions and decisions, in particular:

- To protect legal and other rights of staff or those affected by those actions
- To facilitate audit or examination
- To provide credible authoritative evidence

Quality – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed - through yearly audit.

Accessibility – that records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the Trust – through yearly audit.

Security – that records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled and audit trails will track all use and changes.

Duties and Responsibilities

Chief Executive (CE)
The CE is responsible for the quality of records management within the Trust to ensure compliance of the DP legislation and responsible for managing and monitoring the risks associated with the quality of health records.

Caldicott Guardian (CG)
The CG is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of Personal Confidential data (PCD) are in place.

It is also their responsibility for representing and championing IG and have a fundamental role around confidentiality; justifying and testing that the Trust and partner organisations satisfy the highest practical standards for handling PCD, and ensuring information is shared only for justified purposes, and that only the minimum information is shared.

Senior Information Responsible Officer (SIRO)
The SIRO is reportable to the Board for ensuring that all Information risks are recorded and mitigated where applicable. .
The Trust is subject to a number of legal, statutory and good practice guidance requirements covering records.

All staff members, volunteers and persons acting on behalf of the Trust

- All employees have a responsibility for any records that they create or use. Thus any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.
- Staff must attend relevant training covering records management.
- Staff must refer any concerns and incidents to their manager.

- This responsibility will be set out in all job descriptions.

Training
All managers and staff responsible for records will receive training covering records management at least annually. This is delivered by the Education and Workforce Development Team (EWDT) to support the DSPT and NHSLA Risk Management Standards.

To comply with legislation, this training will follow the HORUS principles:
- holding information securely and confidentially;
- obtaining information fairly and efficiently;
- recording information accurately and reliably;
- using information effectively and ethically;
- sharing information appropriately and lawfully

Management of Records
Records are created so that information is available within the Trust to:
- Deliver the services offered by the Trust to the community.
- Ensure that appropriate records are kept for the operation of the business and are correctly identified and managed.
- Support day to day business which underpins decision making and the delivery and continuity of care.
- Support evidence based practice.
- Meet legal requirements, including requests from patients under DP legislation.
- Assist medical and other audits.
- Support improvements in quality through research and also to support archival functions by taking account of the historical importance of material.
- Assist the Trust in defending any legal claims against it or its staff.

The following is considered unacceptable practice;
- Delete or erase notes, such that the entry is no longer legible.
- Use “white out” correction fluids in any part of a paper record.
- Change original entries, other than as specified above.
- Change entries made by another person.
- Amend the record of an opinion or judgement recorded by a healthcare professional, whether accurate or not, because the recorded opinion or judgement is essential for understanding the clinical decisions that were made and to audit the quality of care.

Naming Folders, Files and Documents
Naming conventions are standard rules to be used for naming both documents and electronic folders. Corporate standards must be followed in the naming of files and folders. It is unacceptable for any documents to leave the Trust without it showing the Trust as being the owner of such documents.

Version Numbers
Where the record is likely to be replaced in the future by a new version, e.g. a policy, a version number should be included, both in the filename and also the document itself,

Structuring Folders and Files
A well thought out structure of folders (also known as directories or classification schemes) for filing documents is a key element to efficient electronic record keeping. Folder titles should be clear and concise and adequately describe the contents.

Access to folders can be set up with varying degrees of permissions / controls, depending on the nature of the contents and who requires access.

Where to Save Documents
There are generally two main areas where documents can be saved – either shared or personal folders. Both of which are located on the network.

Storage of records
All records must be kept securely in storage. When drawn out, the individual user must keep the records in a secure manner in their workplace.

All record storage systems must have in place an effective tracking system in the form of a records inventory which will aid easy retrieval should the record be required.

Transportation of Physical Records
It is recognised that records, both electronic and paper based, should not be taken off Trust premises. However, it is acknowledged that there are operational reasons for doing so. These include transporting records between premises via the internal courier service, or for clinicians with an operational need to take the records between sites personally.

Only such notes as are necessary for those purposes may be taken, and they must remain with the individual at all times. If there is a need to transport clinical records staff are to ensure the process is as safe as possible.

If minimal paperwork is required, it is recommended the NHS Number only is used to ensure the security of any PCD and protect the identity of the patient should any papers become separated?

Leaving records in an unattended private vehicle would require a justifiable reason. Where such justification is thought to exist, the records must be out of sight, for instance in the boot, and the vehicle locked.

Sending Records by Post
This section applies to internal post, external post such as the Royal Mail and any other postal or courier / delivery service.

All records relating to vulnerable children, children in need, children subject to a child protection plan and looked after children must be sent via the Child Health Department.
The records must have been seen by the Designated / Named Nurse for Child Protection before leaving the Trust. They must contain a transfer out summary, and be sent by special delivery to the Child Health Department of a receiving NHS organisation.

If records are to be sent by post, they must be in a robust secure, sealed envelope, clearly marked **"OFFICIAL: SENSITIVE - PERSONAL**" and sent securely by the most appropriate method pertaining to the content

Corporate records relating to commercially sensitive must be in appropriately addressed in a secure, sealed envelope, clearly marked "OFFICIAL – SENSITIVE: COMMERCIAL" and sent securely by the most appropriate method pertaining to the content. The envelope must be robust and sealed to withstand transit through the postal system.

Electronic Transmission of PCD
Computers with access to patient data, whether standalone or networked, must have security measures in place to prevent unauthorised access. Regular audits will be conducted to ensure compliance. Action will be taken against staff that have accessed information that they do not have a legitimate relationship with.

Retention, Archiving and Disposal Procedure for Records

There is a strict process for the retention and disposal of clinical records to ensure compliance with legal obligations, operational, research and safety reasons. In addition to this, the process allows the Trust to effectively manage the storage space available.

Appraisal process
If the records are no longer required, the records will either be securely stored onsite or transferred to off-site storage or disposed of in line with the records retention period pertaining to the type of record.

Archiving
Records that require regular and easy access can be retained on site in individual Directorates. All records retained at base must be secured in a lockable filing cabinet or a secure cupboard/records room.

Archive Year
For all records the archive year is the calendar year in which the last entry was made. The destruction date is the appropriate number of years pertaining to the relevant type of record,

Destruction of Records
All confidential waste must be placed in the allocated “Shred-it” consoles where this applies or shredded confidential waste can go out with normal recycling, Shredding equipment within departments must be a Cross-Cut or Confetti-Cut Shredder with a minimum Din level 3.Non-confidential waste can be placed in the cardboard recycle bins.

Retention of Records
All records are retained for a minimum period of time for legal, operational, research and safety reasons and will depend on the type of record. A record can only be destroyed when it fulfils the following criteria

- last contact with the Trust is over the minimum period for that type of record
- Method of destruction and certificate (where applicable) unless under contract

Permanent Preservation
Records which seem likely to provide material for research or have historical value should be scrutinised with a view to transfer to an ‘Approved Place of Deposit’ located at the Lincolnshire Archives, St Rumbold Street, Lincoln. LN2 5AB.

Destruction certificates should be retained to provide legal proof of destruction in case the records are subsequently requested for subject access or litigation purposes,

Missing Health Record Procedure
When records are mislaid or missing this may be due to;

- Record with Medical Secretary or staff unable to retrieve the record
- Record not tracked or misfiled or patient unable to locate patient-held record

When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of all actions taken.

Sharing Records
All staff should work towards rationalising record collections through sharing records and the information they contain (subject to legal and NHS constraints).
Important points:

- Data belong to the Trust and not to individuals or departments
- NHS records are public records and the CE is ultimately responsible

- The Trust recognises that there are restrictions on the disclosure of information

Confidentiality and Security of Records
The storage, distribution, use and disposal of records will conform to relevant legislation e.g. Data Protection Act 2018, Freedom of Information Act 2000 and ISO 27001:13 – Information Security, and NHS guidance such as, Caldicott Principles, NHS Code of Practice on Confidentiality 2003, and local policies, taking into account best practice.

Records Audit
A Records Audit will be undertaken annually and will consist of an audit of electronic records. The Trust promotes a paper-light / paperless environment for Health Records.

In accordance with requirements defined within the NHS Litigation Authority (NHSLA) and the Care Quality Commission (CQC), the Trust is required to review their record keeping standards annually.

The audit will:

- Identify areas of operation and identify which procedures and/or guidance should comply with this policy.
- Follow a mechanism to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan.
- Set and maintain standards by implementing new procedures, including obtaining feedback where non-conformance to the procedures is occurring and recommend a tightening of controls and adjustment to related procedures.

Clinical Diaries
The use of paper clinical diaries within the Trust is prohibited due to the risk of loss and the introduction of mobile working to access clinical data offline whilst working in the community. Any staff member found to breach this will be subject to disciplinary procedures and notification to Practitioner Performance.

Monitoring

This will be monitored by an annual review of a records audit. Incidents relating to records will be monitored through the Incident Reporting Policy.

Serious incidents i.e. loss of records, misidentification, breaches of confidentially, failure to comply with DP legislation will be subject to further investigation which may include a Root Cause Analysis investigation. All such incidents will be reported following the IG Incident Reporting process.

ACCESS TO INFORMATION (SARs)

This gives direction to staff about the provision of Access to Health Records for data subjects and their representatives and applies to all health records held by the Trust and also applies to entries made by health professionals in records for integrated services.

The main legislative measures that give rights of access to health records include:

- **Data Protection Legislation** – rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf.
- **The Access to Health Records Act 1990** – right of access to deceased patient health records by specified persons.
- **The Access to Medical Reports Act 1988** – right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes

UK legislation sets out 6 principles concerning personal data. The Trust will always strive to ensure that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Not be kept for longer than necessary for the specified purpose.
- Processed in a manner that ensures appropriate security of the personal data.

Duty of Confidence
All those working for or with the Trust, who record, handle, store or otherwise have access to health records have a common-law duty of confidence. All employees have a duty to maintain professional ethical standards of confidentiality.

Any health information, given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else.

There will be cases where information about a patient may need to be shared with a third party, even when consent by the patient or their representative has been refused or where a patient does not have capacity to consent. Where requests for information are received by the Trust, they should always be considered on a case by case basis.

Access to Information Team (AIT)
All staff are reminded that all requests for information made under UK legislation must be handled by the AIT unless otherwise advised by the Data Protection Officer (DPO).

Access by Patients

- A patient, or their representative with patient's consent, has the right to apply for access to their health records. Requests must in writing. Where a patient seeks access to their own record, the Trust should ensure that sufficient identity checks are undertaken to ensure it is satisfied the patient is entitled to the records. These circumstances include:
- Where to release the information could cause mental or physical harm to the patient or others
- Where access would disclose information relating to or provided by a third party who has not consented to that disclosure.

Access by a Patient's Representative
If a request is received from a patient's representative (provided the patient has capacity) the patient is the only person allowed to authorise the release of their record. The representative may include any person the patient consents to have access to their record but not limited to;

- Patients relative, a friend or Litigation friend
- Solicitor or other legal representative

If a patient is unable to authorise the release of their record due to a lack of mental capacity then a person who has been legally appointed to act on the patient's behalf has the right to apply for access to the health record of the patient.
This may include:

- A person holding a Lasting Power of Attorney (LPOA) for health and welfare
- A person holding an enduring Power of Attorney (POA) for Health and Welfare
- An independent Mental Capacity Advocate (IMCA)

Where a request is received from a legally appointed representative, they should be asked to produce evidence that they hold a LPOA which allows the person to make decisions regarding health and welfare. A POA must be registered with the Office of the Public Guardian.

There may also be occasions where a representative (such as a family member) who does not have an automatic right of access to the record, seeks disclosure. Whilst there is no right for next of kin to review the records of an incapacitated patient, there may be circumstances where it is appropriate. Where requests of this nature are made, they must always be considered on a case by case basis and should be referred to the AIT.

The Court of Protection can also appoint deputies for this purpose. This may entail giving access to relevant parts of a patient's records unless the health professional can demonstrate this would not be in the patient's best interests.

Access to a Patient's Record by other Agencies
There will be occasions for requests for access to patient records from other Agencies. These may include the Coroner, Police, General Medical Council, Social Services and other NHS organisations.

The Trust will consider carefully when information can be shared with other agencies and whether consent from a patient can and should be taken beforehand.
Where requests are received from a third party, the Trust will consider the request carefully and on a case by case basis. Request of this nature for records should always be handled by the AIT.

When Police approach staff for information
When a Police Officer makes a request for the information of a data subject, (DS) the request must first be validated by the Access to Information Team (AIT) and disclosed under the following circumstances:

- With the appropriate consent of the patient has been received
- Where the DS has not consented a valid form has been received from the police and signed by the appropriate officer. This may be for;

a. Police and Criminal Evidence Act 1984 – Sections 19 & 20.
b. Terrorism Act – Sections 19 & 39.
c. Fraud Act 2006 – Section 1
d. Computer Misuse Act – Section 1 now the Police and Justice Act 2006 section 35
e. Serious Crime Act 2007 – Section 68 & 72
f. Except for exceptional circumstances as defined by the AIT the information can be released.

Other occasions where we may be able to release without consent are;

- Whether there is a threat to public health and safety
- Whether there is a risk of death / serious harm to the DS or other individuals
- Any order of a Court
- The circumstances of the matter under investigation;
- If the public interest in the specific circumstances outweighs the individual's right to privacy e.g. in 'distress' cases i.e. reported missing person

For the above points approval must be sought from the DPO or IG Lead.

Access to Health Records of a Deceased Person
This is governed by the Access to Health Records Act (1990). Under this legislation where a patient has died, their Personal Representative, Executor, Administrator or anyone having claim resulting from the death has the right to apply for access.

The personal representative is the only person who has an unqualified right of access and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

If a requestor wishes to make a complaint following completion of their request these must be directed to the DPO to handle in the first instance. If the complaint cannot be resolved the requestor must be directed via the Trust complaints procedure.

Response Targets
The UK legislation requires the Trust to complete all request within one calendar month and in exceptional circumstances if it is not possible to comply within this period then the applicant must be informed. This can be extended to a further calendar month under advice from the DPO.

Requests From Outside the UK
Requests from patients living outside of the UK should be treated the same as requests from within the UK.
SCANNING DOCUMENTS

Legal Admissibility (LA) is a core Records Management principle and if a document is scanned and it must be a true representation of the original.

The Trust has a duty to ensure documents created or scanned, stored and migrated through electronic systems meet the evidential weight as outlined in the Civil Evidence Act 1995 to ensure BS 10008 LA should a Court require it

Compliance within does not guarantee LA. It is possible to maximise the evidential weight of a record/document by setting up authorised procedures and being able to demonstrate in court that those procedures have been followed.

Procedures are defined which need to be implemented in order to comply. To demonstrate that it complies with the five principles of information management.
They are:

- Recognise and understand all types of information
- Understand the legal issues and execute 'duty of care' responsibilities
- Identify and specify business processes and procedures
- Identify enabling technologies to support business processes and procedures
- Monitor and audit business processes and procedures

Statement
This is applicable to any Trust system that stores information electronically and its outputs. It covers aspects of the information management processes that affect the use of information in normal business transactions.

This is to establish guidelines for:

- Authenticity and Integrity of stored data
- LA of scanned, stored and electronically communicated data

The purpose is to:

- Provide guidance on process, procedure, audit in order to ensure authenticity, integrity, security and LA of scanned, stored or migrated information
- Improve reliability of, and confidence in, communicated information, and electronic documents to which an electronic identity is applied
- Maximize the evidential weight which a court or other body may assign to presented information
- Provide confidence in inter-organisation information sharing
- Provide confidence to external inspectors (i.e. regulators and auditors) that the Trust's information and business practices are robust and reliable

The requirement to authenticate electronic documents that have evidential significance to a Trust may be vital to continued operations.

Information security is key when discussing LA issues and is the authenticity of the stored information in the form of robust audit trails that evidence;

- When the electronic information was captured, was the process secure?
- Was the correct information captured complete and accurate?
- During storage, was the information changed in any way, either accidentally or maliciously?
- What was the process for scanning paper originals into the system? Can the Trust evidence the quality and integrity of the original document has been maintained?
- Information security implementation and monitoring are key to demonstrating authenticity.

It is essential at the planning stage to consult with appropriate third parties who will need to use, inspect or have a material interest in the results from authenticated systems. Examples of such third parties are:

- Receiving Parties, Auditors, Legal Experts, Technical and Operational Staff and The Courts

The Trust should be aware of the value of its electronic identity management systems, and execute its responsibilities to those systems under the duty of care principle.

To fulfil its duty of care obligations, the Trust should:

- Be aware of and demonstrably comply with legislation and regulatory bodies
- Establish a chain of accountability and assign responsibility for all relevant activity
- Keep abreast of developments with the appropriate bodies and organisations

Training
Training needs of staff will vary according to the local scanning processes and procedures constructed to underpin local service needs.

Process
This applies to information scanned and electronically stored within an Information System and will provide guidance to ensure authenticity, integrity of in regards to LA.

The purpose of the process is to ensure:

- Authenticity and Integrity of stored data
- LA of scanned, stored and electronically communicated data
- Improve reliability and confidence in communication in electronic documents.
- Provide confidence in inter-organisation information sharing

Type of Document
Identify documents for scanning. Check for ultra-shiny fax paper - this will not scan properly and needs to be photocopied before being scanned.

Duplication
If duplications are found these should be destroyed and not form part of the scanned document. Any handwritten information that has been added after the date of the original document should be retained and scanned.

Misfiling
Check that all the information in the document pertains to the same patient (NHS No: Name and DoB). If misfiled information is found it must be relocated to the appropriate record.
Quality of Original or Photocopy
If the original document is of poor quality, it is unreadable and photocopying and/or enhancing does not improve the readability, a note should be placed on file stating **'Parts of this document were unable to be scanned due to the poor quality of the original'.**

Images
Image processing is a post scanning technique to improve the quality of a scanned document. There may be good reasons for improving image quality but it is **NOT** permitted for clinical photography in case essential detail is removed.

Images may be stored as a JPEG or Bitmap, TIF or GIF but storing as a file is recommended as it will help to retain the integrity of the image.

Quality Control
It is important to be able to demonstrate to a court that the quality controls are adequate and work. A check should be made of the paper document against the scanned document, ensuring that:-

- The same amount of pages has been scanned, pages are legible and exact replicas

Retention
No original documentation should be destroyed until quality checks have taken place and assurance the scanned documents are legible and stored securely.

Audit
The audit trail as a minimum will log details of each significant event in the life of the document within the system. The audit rail will be generated by the system of the user, date and time and stored securely within a user's access role.

Security and Protection
Security and protection covers user access which will capture details about the User, Date and time of scanning took place.

Document Deletion
To meet DP it may be necessary to amend or delete documents or parts of documents which will be identified via the system audit trail.

NHSLA Monitoring

Minimum requirement to be monitored	**Process for monitoring e.g. audit**	**Responsible individuals/ group/ committee**	**Frequency of monitoring /audit**	**Responsible individuals/ group/ committee (multidisciplinary) for review of results**	**Responsible individuals/ group/ committee for development of action plan**	**Responsible individuals/ group/ committee for monitoring of action plan**
DSPT Standards	Review / Audit / Reports	IG Lead	Annual	IG Lead / IGMAG	IG Lead / IGMAG	IG Lead / IGMAG

Equality Analysis

A.	Briefly give an outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be	To provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.
B.	Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? **Please give details**	All Staff and Service Users

C.	Is there is any evidence that the policy\service relates to an area with known inequalities? **Please give details**	No		
D.	Will/Does the implementation of the policy\service result in different impacts for protected characteristics?	No		
		Yes	No	
	Disability		X	
	Sexual Orientation		X	
	Sex		X	
	Gender Reassignment		X	
	Race		X	
	Marriage/Civil Partnership		X	
	Maternity/Pregnancy		X	
	Age		X	
	Religion or Belief		X	
	Carers		X	
	If you have answered 'Yes' to any of the questions then you are required to carry out a full Equality Analysis which should be approved by the Equality and Human Rights Lead – please go to section 2			
The above named policy has been considered and does not require a full equality analysis				
Equality Analysis Carried out by:		Kaz Scott, IG Lead		
Date:		June 2018		