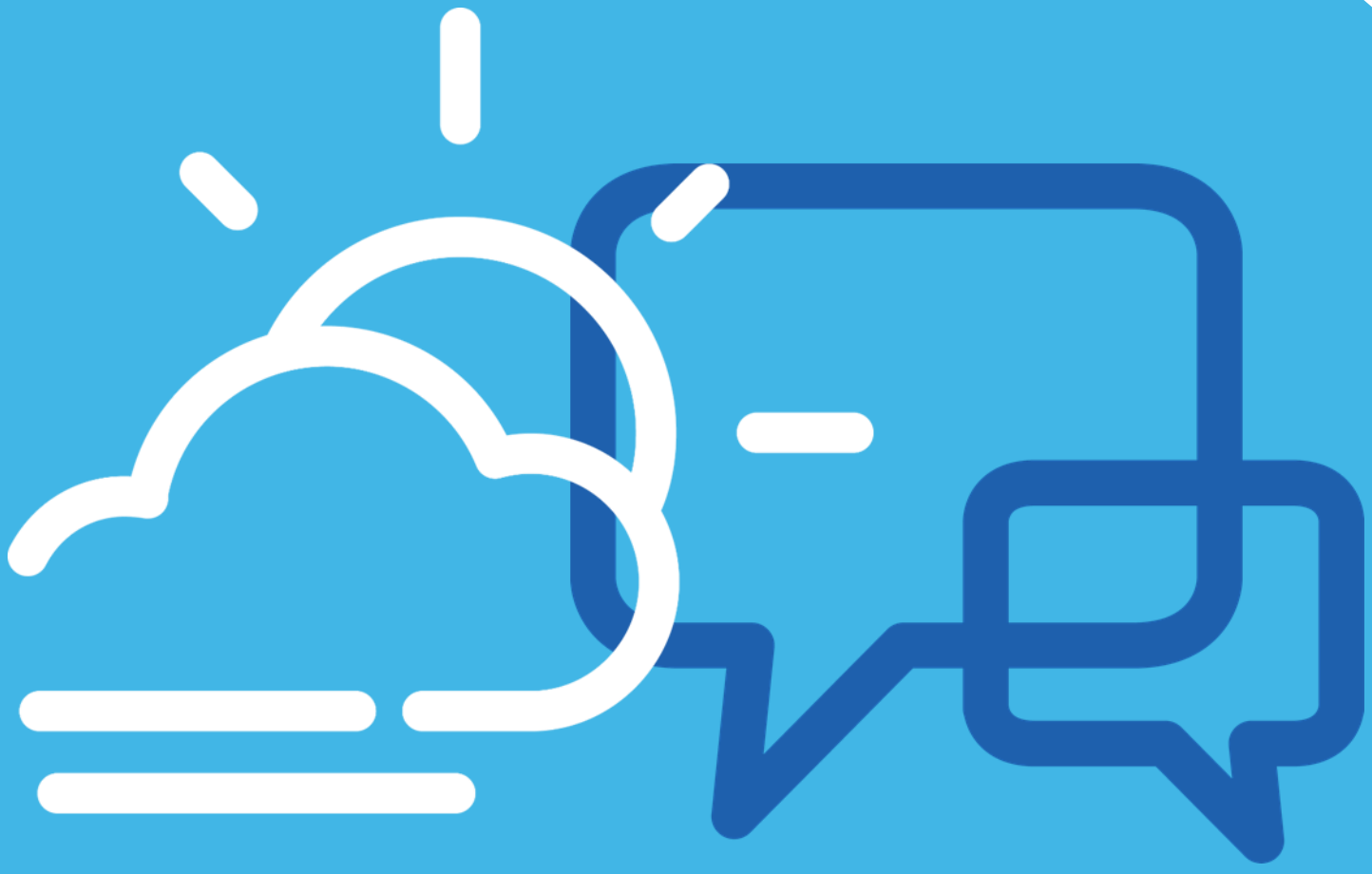
NHS
Greater Manchester Mental Health
NHS Foundation Trust

# Confidentiality Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

| | |
|---|---|
| **Document Name:** | **Confidentiality Policy** |
| **Executive Summary:** | This policy identifies how Greater Manchester Mental Health executes its duty to keep client and staff information safe and confidential whilst, at the same time, not compromising its ability to share information where it is needed. |
| **Executive Lead:** | Director of Finance, Capital & IM&T |
| **Document Author:** | Deborah Tonkin (Information Governance Manager)<br>Deborah.tonkin@gmmh.nhs.uk |
| **Document Purpose:** | Policy |
| **Target Audience:** | All employees of Greater Manchester Mental Health NHS FT |
| **Additional Circulation List:** | All employees via the Trust Intranet |
| **Date Ratified:** | 15/01/19 |
| **Ratified by:** | Information Governance Steering Group |
| **Consultation:** | This version was circulated for comments via the information governance steering group prior to ratification. |
| **Cross Reference:** | Related Trust policies and procedures including all Information Governance Policies |
| **Superseded Docs:** | Confidentiality Policy IG03 V1 |
| **Date of Equality Impact Assessment:** | February 2017 |
| **Board Objective Reference:** | Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes<br>Objective 3 – To engage in effective partnership working<br>Objective 6 – To achieve sustainable financial strength and be well-governed |
| **CQC Regulation Reference:** | Regulation 11: Consent<br>Regulation 17: Good Governance<br>Quality & Risk Profile |
| **Risk Register Reference:** | N/A |
| **Contact Details for further information** | Information Governance Manager<br>Tel: 0161 358 1573<br>Deborah.tonkin@gmmh.nhs.uk |
| **Document Status** | This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy. |

## Contents

# 1. Introduction

This policy sets out to identify how Greater Manchester Mental Health NHS Foundation Trust executes its duty to keep client and staff information safe and confidential whilst, at the same time, not compromising its ability to share information where it needed.

## 1.1. Purpose

All staff employed by the Trust have a duty to keep such information strictly confidential and use it only for the proper purposes in accordance with the law. This is especially pertinent to the General Data Protection Regulation, Data Protection Act 2018, the NHS Guidance, (the Caldicott Principles), and Trust policies. Good practice requires all organisations having access to client/staff information to do the following:-

- Justify the purpose.
- Use client identifiable information only if absolutely necessary and legally permissible.
- Ensure that all information is accessed only on a strict need to know basis.
- Ensure that everyone with access to identifiable information is aware of their responsibilities.
- Understand and comply with the law.

It is crucial that all staff understand the reasons and legal basis for processing personal identifiable information. This policy will describe the purpose of obtaining sensitive information from service users, the principles to follow to safe-keep the information provided in confidence, circumstances when this information may need to be shared, disclosed or accessed and will signpost staff to relevant procedures.

# 2. Definitions

**'Confidentiality'** applies to information whether received through formal channels (e.g. in a formal report), informally or discovered by accident. It applies to Trust business, employees and potential employees, clients or individuals or organisations who come into contact with the Trusts data i.e.

- Third parties
- External contractors
- Voluntary Organisations

Information which can be classed as 'confidential' can broadly be grouped in the following areas:

**Patient Data – Special Category data**

– race;

- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

**Corporate Information**
Information about the trust such as how decisions are made, budgets, spending etc.

## 2.1. Special Category data

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9 also.

This is because special category data is more sensitive, and so needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others. Under GDPR fines of up to 20 Million euros or 4% of turnover can be levied and criminal convictions imposed on the individual responsible.

## 2.2. Corporate information

This may be used to damage the Trust and other organisations, as well as individuals or Trust staff. It may be prejudicial to the business of the Trust, used to threaten the security or property buildings and systems.

## 2.3. Breaches in confidentiality

This happens when sensitive information is given to/accessed by people who are not authorised to access it. They are most likely to happen when procedures have not been agreed or followed.

They can also happen when information is passed between sections, departments or organisations, or when information is being stored.

Individuals who access data without the authorisation or justification to do so can be

levied with personal fines and criminal convictions. It is viewed as gross misconduct by the Trust and could result in dismissal.

### 2.4. General Data Protection Regulation

The General Data Protection Regulation (GDPR) applies across Europe from 25th May 2018.

GDPR strengthens the rights of individuals to control how their personal data is processed. It places tighter obligations on organisations to be more accountable for data protection.

### 2.5. Data Protection Act 2018

The Data Protection Act 2018 supersedes the Data Protection Act 1998.

## 3. Duties

### 3.1. Board/Lead Committee

The Information Governance Steering Group is responsible for the approval and monitoring of this Policy.

### 3.2. Chief Executive

The Chief Executive has ultimate responsibility for ensuring that the Trust develops and implements robust confidentiality procedures. This role has delegated responsibility to the Associate Director of Finance and IM&T who is the Senior Information Risk Officer (SIRO).

### 3.3. Caldicott Guardian

The Caldicott Guardian is the appointed senior clinician who carries the ultimate responsibility to oversee the use and sharing of patient identifiable and clinical information. This is a key role in ensuring the Trust satisfies the highest practical standards for processing patient identifiable information. Acting as the 'conscience' of the Trust, the Caldicott Guardian actively supports work to facilitate and enable information sharing and advices on options for lawful and ethical processing of information as required.

### 3.4. Data Protection Officer (DPO)

The GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and on organisations that carry out certain types of processing activities.

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO). The DPO must be independent, an expert in data protection, adequately resourced,

and report to the highest management level.

The Trust's DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

### 3.5. Head of IM&T Service Delivery

The Head of IM&T Service Delivery is responsible for the strategic and operational management of the Information Governance agenda.

### 3.6. Information Governance Manager

The Information Governance Manager is the Trust lead for the annual Data Security and Protection Toolkit self-assessment. The IG Manager supports the Caldicott Guardian to ensure the Trust meets the highest standards for appropriate handling of patient information in accordance with the Care Quality Commission regulations The Information Governance Manager is responsible for overseeing day to day issues regarding patients' confidentiality; developing and maintaining policies, standards, procedures and guidance and raising awareness when necessary.

### 3.7. Clinical Academic Group Directors and Senior Managers

All Directors and Senior Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local process and that there is on-going support.

### 3.8. All Employees

All employees, whether permanent, temporary, contracted or a third party accessing GMMH data are responsible for ensuring that they are aware and respect the confidentiality of GMMH data and they know the requirements incumbent on them and for ensuring that they comply with these on a day to day basis.

Most importantly, all Trust employees have responsibility to act professionally in order to meet the confidentiality standards outlined in this policy. This is a legal and professional obligation, which is also set out in Trust employment contracts.

### 3.9. All Staff and third parties with access to GMMH data

All staff must ensure that:

- service users are aware when their information is recorded or health records are accessed;
- the Trust's Privacy Notice and information leaflets on patient confidentiality and information disclosure are available for service users and have been read and understood;
- service users know when information may be shared with others;
- service users understand that their information may be shared with third parties in order to deliver health care (under GDPR this does not

require consent);

- they are facilitated in exercising their rights to have access to their health records;
- rights of service users are respected;
- service users concerns and queries are answered.

## 4. Processes and Procedures

### 4.1. Using and Disclosing Confidential Information

All staff must ensure that they are aware of the legal basis for which to share data and must not disclose outside of these parameters without prior approval from the Caldicott Guardian or Data Protection Officer.

### 4.2. Legal Considerations

There are four main areas of law which constrain the use and disclosure of confidential personal health information. These are briefly described below.

### 4.3. Common Law Duty of Confidentiality

This is built up from case law where practice has been established by individual judgements. The key principle is that information provided in confidence should not be disclosed further, except as originally understood by the confider, or with their subsequent permission.

Whilst judgements and other relevant legislation have established that the duty of confidentiality can be overridden 'in the public interest', these have centred on case by case consideration of exceptional circumstances.

### 4.4. General Data Protection Regulation and Data Protection Act 2018

The General Data Protection Regulation sits within the Data Protection Act 2018. It is the legislation that provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers all staff records.

There are six principles identified under GDPR that set out standards for information handling and sets the foundation for personal data to be:

1. Lawful, fair and transparent
2. Limited for its purpose
3. Adequate and necessary
4. Accurate

5. Not kept longer than needed
6. Integrity and confidentiality (security)

GDPR also details a separate accountability principle which details organisations' responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance.

## 4.5. Human Rights Act 1988

Article 8 of the Human Rights Act (1988) establishes a right to respect for private and family life. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the General Data Protection Regulation and the common law duty of confidentiality should satisfy Human Rights requirements. There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

## 4.6. Access to Health Records Act (1990)

The records of deceased persons are protected by the provision of the Access to Health Record Act (1990). These apply only to health records created after 1st November 1991. Where a patient has died, records created after the said date may only be accessed by the following:

- The legal personal representative of the deceased i.e. the executor of the deceased's will or (where there is no will) the administrator of his/her estate.
- A person with a possible claim arising out of the death of the patient. The claim does not need to be against the Trust. It may, for example, be an insurance claim. In this case the person is entitled only to such information as is relevant to the potential claim.

It should be noted that if the deceased patient gave a written instruction that any of the above were not to see his/her records, such instruction overrides the rights contained in the 1990 Act and must be respected.

There are no rights of access to records created before 1st November 1990 and the usual rules of confidentiality apply.

## 4.7. Service User Consent to Disclosure of Confidential Information

Under GDPR consent to share data for the purpose of delivering health care is no longer required. However data subjects must be informed of who their data will be shared with and for what specific reason. This will be done via Privacy Notices. There are 6 legal bases for the processing of data, where consent is used as the legal basis the data subject must be informed of their strengthened rights.

## 4.8. Competence to Consent

Seeking consent of service users may be difficult due to illness, disabilities or circumstance that may prevent them from comprehending the likely uses of their information. Mental Capacity Act (2005) is intended to protect people who lack the capacity to make their own decisions. The act allows the person, while they are still able, to appoint someone (for example a trusted relative or friend) to make decisions on their behalf, in their best interest, for their health and personal welfare not just financial matters, once they lose the ability to do so.

## 4.9. Disclosure without Consent

There are only three exceptional circumstances where disclosure without consent in a patient capacity may be justified. These are:

- statute law requires
- there is a court order
- disclosure may be necessary in the public interest where a failure to disclose information may expose others to risk or serious harm.

The courts, including coroner's courts, some Tribunals and persons appointed to hold inquiries, have legal powers to require disclosure of information that may be relevant to matters within their jurisdiction. This does not require the consent of the service user whose records are to be disclosed. Such disclosures must be strictly in accordance with the terms of the court order and should provide the required information to the bodies specified in the order.

Disclosures in the public interest may be necessary to prevent serious crime or risk of significant harm. Public interest is described as exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. **Decisions about the public interest are complex and must take into account both potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.**

Serious crime can be defined as cases involving murder, manslaughter, rape, treason, kidnapping and child abuse which may all warrant disclosure of confidential information in the public interest. Significant harm to the security of the State or public order also fall within this category. By contrast theft, fraud or damage to property where loss or damage is less substantial would generally not warrant a breach of confidence.

Any disclosure of information should be proportionate and limited to relevant details with each case being considered on its own merits. In circumstances where it is difficult to make a judgement, staff should contact the Information Governance Department or seek legal or other specialist advice from the Trust solicitors, the Caldicott Guardian or the Data Protection Officer.

## 4.10. Multi Agency Public Protection Agreements (MAPPA)

The aim of the Multi Agency Public Protection (MAPPA) is to co-ordinate a risk management plan drawn up for most serious offenders from the information, skills and resources provided by individual agencies.

Three groups of people who might be referred to MAPPA are registered sex offenders, all violent and non-registered sex offenders sentenced to 12 months or more in prison (also includes patients on hospital orders) and any other offenders posing a risk of serious harm. The Criminal Justice Act (2003) puts a duty on NHS organisations to co-operate with MAPPA.

## 4.11. Representation at Mental Health Act Tribunals

Care Quality Commissioners, Associate Hospital Managers, Independent Opinion Doctors, Second Opinion Approved Doctors (SOADs), Mental Health Review Tribunal Doctors, Independent Mental Health Advocates (IMHAs), Independent Mental Capacity Advocates, Best Interest Assessors (BIAs), Mental Health Accessors of Deprivation of Liberties (DoLs), solicitors and other legal representatives who are involved in the representation of patients detained under the Mental Health Act (2007) before the Mental Health Review Tribunal (MHRT) require access to medical records.

It is essential that service users' representatives maintain the highest possible standards in the preparation, presentation and conduct of their client's case before the Tribunal. These representatives have a general duty at all times to act in the best interests of the service user and are under a duty to keep the service users' affairs confidential.

Staff must contact the Mental Health Act Office for further guidance.

## 4.12. Research and Audit

Researchers who have contractual agreements with the Trust may want to use clinical information to conduct scientific projects to improve care and treatment of service users.

All research staff must keep identifiable information secure at all times. Associated researchers should clarify within research proposals the arrangements to obtain permission to access clinical information. Once explicit consent is obtained, researchers can use clinical information to conduct research.

## 4.13. Key Decisions on Confidentiality

The questions below can be used to underpin key decisions on confidentiality:

**Is the disclosure needed to support the provision of healthcare or to assure the quality of care?**
Service users must be informed in advance that some information about them will be shared in order to provide them with complete care and treatment.

**If not for the purpose of healthcare, is the disclosure to support a broader medical purpose such as research?**
This information should be anonymised for research purposes unless disclosure of patient identifiable data is exceptionally justified in the public interest or has temporary support in law under section 251 of the NHS Act (2006).
Under GDPR some research could be legitimate using the legal basis of legitimate interest of the Trust/NHS.

**If the purpose served by disclosing is not healthcare or another medical purpose, what is the basis in administrative law for disclosing?**
The Trust obtains sensitive information from service users for the provision of healthcare services. Information provided in confidence by service users can only be disclosed to other agencies if service user's explicit consent is gained.

**Is disclosure either a statutory requirement or required by order of a court?**
Any disclosure that has either a statutory requirement or court order must be complied with. This disclosure should be limited to required information.

**Is the explicit consent of a service user needed for disclosure to be lawful**?
Unless disclosure of patient identifiable information is required by law courts, is for health care purposes, or is supported by section 251of the NHA Act (2006), for the processing to be legal it must meet one of the other legal bases under GDPR.

The 6 legal bases for processing data are:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, (this cannot apply if you are a public authority processing data to perform your official tasks).

## 4.14. Requests to Access Medical Records

The General Data Protection Regulation defines the right to access personal data by the owner or others that have owner's authority to access this information. The right to access can be limited to a particular section or cover the full set of information held by the Trust. **The Trust is under a legal obligation to disclose the**

**information within 1 month.**

Requests to access confidential clinical information may come from the following:

- current or former service users;
- a representative, (e.g. solicitor, advocate relative);
- a health professional;
- partner agencies;
- the police.

Procedures for staff on how to deal with requests of access to medical records can be found in the Trust policy on Access to Health Records.

The responsibility of authorising disclosure in response to requests to access clinical records lies with the Consultant who provided the most recent episode of care after reviewing the sensitivity of the information and protecting third party information.

## 4.15. Methods of Disclosure

When sharing information, staff must ensure that the information is going to be received by the requestor only. If hard copies of medical records are requested, personal identifiable information should be sent either by an authorised courier or recorded delivery. It is crucial to make sure the parcel is named and addressed correctly.

## 4.16. Incidents involving breaches of Confidentiality and Information Security

Any incident that involves the loss of personal information (on paper or electronic format) must be reported using DATIX. It is the responsibility of the service where the breach occurred to inform the DPO, SIRO or IG team of any high level breach immediately. Reported incidents will be investigated according to the Trust Incident Policy. In line with GDPR, high level incidents will be recorded on the external DS&P website and the ICO informed where required. The ICO must be informed of any incidents within 72 hours.

Information incidents will be reviewed by the Information Governance Team and reported through the Information Governance Steering Group.

## 4.17. Information Governance Serious Untoward Incidents

All staff have a duty to report any breaches of data confidentiality or suspected breaches as soon as is possible.

It is advisable to contact the DPO directly should there be a serious incident.

Staff must not attempt to cover up any data loss as this may expose the Trust and the individual to sanctions from the Information Commissioner's Office (ICO). If the ICO identifies that an organisation has not complied with the General Data

Protection Regulation and disregarded the law, they can impose tough new sanctions under section 55 of the Act. **These sanctions include organisational and personal monetary penalties of up to £18 million or 4% of turnover along with custodial sentences.**

### 4.18. Incidents involving inappropriate access to records

Any concerns of inappropriate access to electronic patient records should reported to the Information Governance Team who will carry out an audit and liaise with the corresponding Information Asset Owner to investigate and involve HR where appropriate.

The Trust uses a proactive audit tool to identify inappropriate access. Once an alert is made via this tool, it is reported to the staff member's line manger to investigate further and involve HR.

Service users can log a complaint about suspected inappropriate access to the Information Governance Department and explain the basis of the concern in writing. They may be required to provide names of people who might have accessed records inappropriately and a time period to guide the investigation. Once the written request is received by the Information Governance Department, an audit of access will be carried out. If there is cause for concern an investigation will be carried out and HR polices followed.

## 5. Training Requirements

All Trust staff must attend the compulsory induction training when they start their employment with the Trust. As per GDPR, all GMMH staff who handle/process personal data must have completed and passed appropriate Data Security and Protection training prior to being granted access to GMMH systems and then annually thereafter.

## 6. Monitoring

| Minimum Requirement | Frequency | Process for monitoring | Evidence | Responsible Individual(s) | Response Committee(s) |
|---|---|---|---|---|---|
| All members of staff are trained accordingly to carry out the requirements of the policy | Annually | Audit | Report | IAOs | IGSG |

## 7. Resource/Implementation Issues

There are no resource service implementation issues.

## 8. Risk Issues

This confidentiality policy will form part of the Trust's overall Information Governance

Assurance framework.

## 9. Requirements, Supporting Documents and References

### 9.1. Requirements

| | |
|---|---|
| **Board Objective Reference:** | Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes<br>Objective 3 – To engage in effective partnership working<br>Objective 6 – To achieve sustainable financial strength and be well-governed |
| **CQC Regulation Reference:** | Regulation 11: Consent<br>Regulation 17: Good Governance<br>Quality & Risk Profile |

### 9.2. Supporting Documents

- Information Governance Policy
- Information Governance Staff Handbook
- Information Security Policy
- Information Sharing Policy
- Freedom of Information Policy

### 9.3. References

- The Access to Health Records Act 1990 Link
- Computer Misuse Act 1990 Link
- Data Protection Act 2018 Link
- General Data Protection Regulation Link
- Human Rights Act 1998 Link

## 10. Subject Expert and Feedback

Advice and support queries in relation to this document should be sent to the author.
Deborah.tonkin@gmmh.nhs.uk Information Governance Manager
Tel: 0161 358 1573

## 11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.