Oxford Health NHS
NHS Foundation Trust

POLICY CONTROL DOCUMENT - 1

POLICY TITLE	**INTEGRATED INFORMATION GOVERNANCE POLICY**
POLICY CODE	**CORP 19**
REPLACES POLICY CODE (IF APPLICABLE)	**IG1-IG17**
AUTHOR (Name and title/role)	**Mark M Underwood, Head of Information Governance**

TRUST BOARD SUB-COMMITTEE WHICH APPROVED ORIGINAL VERSION	
(Name of Committee) **Integrated Governance Committee**	**(Date of approval)** **20 April 2010**
DATE OF NEXT REVIEW	**Q4 2019/2020**

REVIEW HISTORY

COMMITTEE WHICH APPROVED REVISED VERSION	
Governance and Information Management Committee	**DATE 15/09/2010**
Governance and Information Management Committee	**DATE 06/04/2011**
Integrated Governance Committee	**DATE 25/01/2012**
Governance and Information Management Committee	**DATE 21/12/2012**
Information Management Committee	**DATE 22/11/2013**
Information Management Committee	**DATE 27/02/2014**
Information Management Committee	**DATE 15/10/2014**
Information Management Group	**DATE 15/01/2016**
Effectiveness Committee	**DATE 13/04/2017**
Effectiveness Committee	**DATE: 18/01/2019**

CURRENT VERSION PLACED ON INTRANET	**DATE**

CHAIR(S) OF APPROVING COMMITTEE Dr Mark Hancock

SIGNATURE(S) 

TITLE(S) Medical Director.....

DATE .18 January 2019.....

POLICY CONTROL DOCUMENT - 2

NUMBER OF PAGES (EXCLUDING APPENDICES)	
SUMMARY OF REVISIONS: **Review and inclusion of GDPR requirements**	

Approval Checklist	✓
CQC Regulation/NHSLA Standard identified and how the policy meets the standard stated	✓
Consultation process undertaken **Outline with whom: Information Management Group.**	✓
Equality Impact Assessment completed	✓
Has the potential for an impact on a person's human rights been considered	✓
Training implications assessed and agreed where relevant with Learning Advisory Committee	✓
Any resource implications for operational services discussed with the Chief Operating Officer	✓
Monitoring/audit arrangements included	✓

All policies are copy controlled. When a revision is issued previous versions will be withdrawn. Uncontrolled copies are available but will not be updated on issue of a revision. An electronic copy with be posted on the Trust Intranet for information.

Oxford Health NHS
NHS Foundation Trust

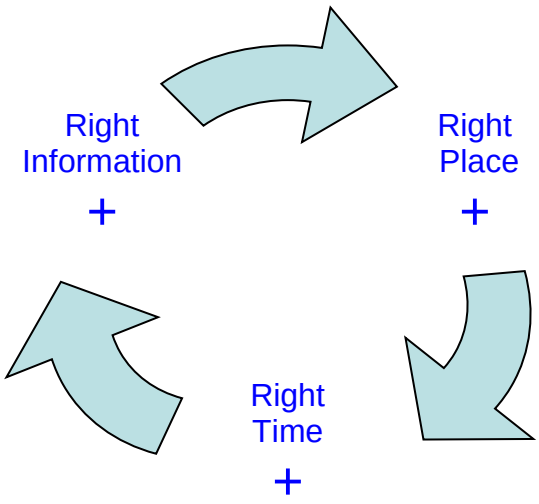
policy	CORP19
review	Q42019/2020

Policy applicable to -	All areas ✓	Specific Areas

Integrated Information Governance Policy

1 Aim of Policy

The aim of the policy is to set out the Trust requirement for Effective Information Governance. Effective Information Governance ensures that the right information is in the right place at the right time.



= EFFECTIVE INFORMATION GOVERNANCE ✓

Effective information governance is essential to delivering our core values of Caring, Safe and Excellent.

Information Governance concerns compliance with the law and the NHS regulatory framework. This includes the security, confidentiality, availability, fitness for purpose and legitimate use of personal identifiable data (PID).

An Individual's rights must be respected and information recorded and used appropriately, legally and accurately.

Information Governance also applies to business or corporate information, where data may not identify individuals.

The Trust needs to collect and use information to function. Information is necessary to support the provision of high quality care to patients and to effectively govern the

organisation. Information contributes to the delivery of caring, safe and effective services, and is necessary to: manage and deploy resources; monitor the quality and performance of services; inform investment decisions; aid communications; provide education and training; and to support research and development activities.

The Trust is committed to high quality practice in the capture, storage, processing, use, and sharing of information. This is at the heart of Information Governance.

The aim of this policy is to ensure that:

→ An individual's rights are respected;

→ Information is available and fit for purpose;

→ Personal information is recorded and used appropriately, legally and accurately;

→ All information and information assets are secure and confidence assured;

→ The Trust complies with the law and the NHS regulatory environment.

The Trust is required to comply with The Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR). Article 5 of the GDPR sets out six principles which are incorporated in the DPA and are at the heart of this policy.

2 Legal and policy framework

- **Human Rights Act (1998)**: all public law is potentially affected by this Act, Article 8 is important for this policy as everybody is entitled to respect for their private and family life, their home and their correspondence.
- **General Data Protection Regulation (the Regulation (EU) 2016/679)**
- ***Data Protection Act (2018)***: relates to the processing (use) of personal information where the subject (person) is identifiable. This is relevant to patient and employee information.
- **Freedom of Information Act (2000)**: allows anybody to ask if the Trust has information, and subject to exemptions to obtain it. This is relevant to corporate information.
- **Mental Capacity Act (2005)**: permits decision making on behalf of a person who lacks capacity, and a decision relating to their information is made in their best interests.
- **Mental Health Act (1983)**: although providing a framework for compulsorily dealing with people who have mental disorder, there are information implications in terms of information sharing and records management.
- **Public Records Acts 1958 and 1967**: sets out what 'government' information should be permanently preserved and made available for public access.
- **Computer Misuse Act 1990**: This legislation has created three criminal offences related to computer systems: unauthorised access; unauthorised access with the intent to commit or facilitate the commission of further offences; and unauthorised modification of computer material.
- **Health Act 2009 and the NHS Constitution**: patients and staff are entitled to privacy and confidentiality and to expect the NHS to keep confidential information safe and secure. The Constitution also incorporates the right of

access to health records, which will always be used to manage treatment in the best interests of patients.

- **Common Law Duty of Confidence**: court made law, the common law, establishes that information provided by an individual to another individual is confidential and consent is normally required to share it.
- **NHS Code of Practice on Records Management:** describing the standards the NHS sets for records management and the length of time different types of records should be kept for records to be. Click Here
- **Confidentiality: NHS Code of Practice**: describing the standards the NHS sets for confidentiality, making decisions about disclosure, information sharing and consent. Click Here
- **Information Security Management: NHS Code of Practice**: describing the standards the NHS sets for information security management. Click Here
- **Pseudonymisation of Patient Information for Secondary Use**; describing the technical requirements for de-identifying information for use in commissioning, contracting, and non-direct care. Click Here
- **Care Records Guarantee**: describing the promise made to patients about how information about them is used. Click Here
- **NHS Protect: Patients recording staff in NHS and Social Care settings**: describing how staff can deal with situations where they are being asked about recording contact or are being recorded by patients. Click here
- **NHS Information Governance - Guidance on Legal and Professional Obligations**: describes best practice guidance on legal issues in health and care information governance. Click Here
- **Care Quality Commission Essential Quality and Safety Standards: CQC Regulation 17**. The Healthcare regulators standards for governance. Click Here

3 Policy

Trust employees *(which includes employees, appointees (for example, Non-Executive Directors), secondees, and volunteers such as Governors and Mental Health Act Managers)* are given access to information, computer systems and equipment to facilitate the execution of their duties. The essential principle of such access is:

'Employees are provided with computing, information and communication facilities for appropriate business use and if such facilities are used inappropriately, employees may be subject to disciplinary action or where appropriate, criminal action'

Effective use of computing, information and communication facilities will be underpinned by employee familiarity with the Trust's Integrated Information Governance Policy. Employees will also need to obtain and maintain competence and skills to use systems and to follow any guidance issued relating to information governance by the Trust. **This Policy is underpinned by the Standard Operating Procedures which comprise the Integrated Information Governance Policy Procedures and Guidance.**

Any other authorised users of Trust information or systems are subject to the terms of this policy. Breach of the policy may result in terminating their use.

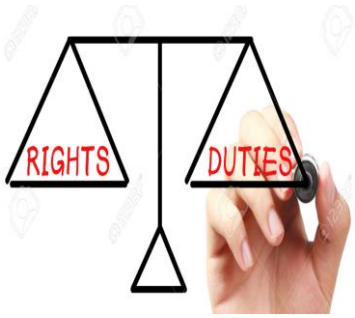
The Trust will put in place a comprehensive and effective system of internal control, which supports this Policy. The internal control framework will consist of Procedures, Guidance, System Controls and Assurance incorporating:

- Policy, procedures and guidance;
- Awareness raising and formal training;
- System controls and assurance;
- Testing and monitoring compliance and the effectiveness of controls.

  (These are listed in Appendix B of this policy)

The Information Governance policy of the Trust is to:

1. Respect individual rights;
2. Use information confidentially and securely;
3. Protect the Trusts information and communication technology infrastructure;
4. Obtain information fairly and record efficiently;
5. Record information accurately and reliably;
6. Use information effectively and legitimately;
7. Share information appropriately and lawfully; and
8. Encourage best practice

1. Respect individual rights	
	*Lawfulness, fairness and transparency: The Trust must comply with laws which govern personal information and corporate information. The Data Protection Act and General Data Protection Regulation provides a legal framework about information about people which the Trust must follow. The Freedom of Information Act allows people to request information about the Trust, including activities, structures, committee papers and contracts for instance. When we use information about people we must also consider confidentiality, which is a common law principle, and means for the most part we can use information about people with their consent but must have other legal justification to use information without consent.*

The Trust, and hence employees of the Trust, must comply with the law. A number of laws affect information about people and information about the Trust. The Data Protection Act concerns processing information that people can be identified from. The common law duty of confidence must also be considered. Article 8 of the Human Rights Act provides that everyone has the right to respect for his private and family life, his home and his correspondence. The Freedom of Information Act concerns information about the Trust and any person can make a request to obtain organisational information.

Principle A of Article 5 of the GDPR states that ”Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)”.

Fair Processing: This means that the Trust must publish a Privacy Notice and our employees must tell patients that the Trust collects personal information about them.

The duty also applies to line managers who must tell employees that the Trust collects personal information about them. In both cases a record must be made of the discussion. Primarily the Trust will use:

- → Information identfying people where is a legal basis for doing so;
- → Information with the person's consent (there are exceptions provided for in law which are discussed in guidance);
- → Information to aid the provision of healthcare to an individual;
- → Information for employee administration;
- → Information for health and social care management and administration;
- → Information for clinical audit, surveys or research purposes;

And the Trust will make arrangements so that:

- → People can apply for access to their information, (called a Subject Access Request);
- → The Trust looks after personal information and uses it appropriately.
- → A notification is made to the Information Commissioner's Office (ICO), which states the particular purposes personal information is used for.

Respecting people's rights by complying with fair processing and Article 5 *Principle **A*** of the GDPR, supported by good information governance practice, will also ensure compliance with *Chapter 3 of the GDPR,* which requires the Trust to produce and make available: Transparent information, communication and modalities for the exercise of the rights of the data subject. The Trust must ensure that personal data is processed in accordance with the rights of data subjects and information the Trust makes available shall be concise, transparent, intelligible and in an easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means

Subject Access Requests: The Trust will respond to requests for access to records by patients, employees, or authorised others (called subject access requests) and where appropriate will provide copies of records to patients in accordance with the Data Protection Act.

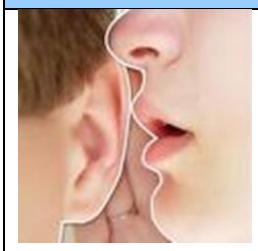
Copying correspondence: The Trust will provide copies of correspondence to patients unless it is not appropriate to do so or the patient does not wish to receive them.

Projects, services, systems or initiatives which include or are likely to include use of personal information must consider information governance issues. This will include the considerations of data protection by design and conducting a data protection impact assessment (DPIA). Due diligence must also be completed and a data processor agreement will be required where personal information is being processed by a third party.

Recording sessions: Patients and others may request recording or filming clinical or other sessions they are involved in. The Trust will agree to such requests generally unless there are compelling clinical, risk or safety, safeguarding, privacy and dignity or any other considerations or reasons which make such a request impracticable.

The Trust may photograph, record or film care or treatment for clinical, research, educational, teaching, or clinical governance purposes. The Trust will explain the purpose to patients and obtain consent to do so where practicable.

The Trust is required to respond to any requests for information made under **the Freedom of Information Act**. The Act also requires the Trust to maintain a Publication Scheme, and this is available on the Trust website. The Trust must also notify the Information Commissioner that it holds information and has a publication scheme. By necessity the Act and the GDPR requires the Trust to employ adequate records management standards.

2.	**Use information confidentially and securely**
	*Integrity and confidentiality: Confidentiality is a primary consideration when we use information about people. The common law duty of confidence comes from judge, court and tribunal decisions. This means for the most part we can use information about people with their consent but must have other legal justification to use information without consent. It is also essential that we protect confidential information and keep it safe and secure. Patients and staff are assured that we look after information about them and use it with consent for the purposes described to them.*

Confidentiality: The provision and specified use of confidential information is at the heart of effective healthcare.

- → Information should not be disclosed or used for any other purpose beyond the health care of that individual without the explicit consent of that patient.
- → There may sometimes be a legal reason for disclosure without consent (a Court order, Police proceedings, or a Child Protection issue, for example), or there may be a significant risk to the patient or to others that outweighs the duty of confidence.
- → Employees may only access patient information where it is necessary and they have established a legitimate clinical relationship with the patient (this is a clinical or approved relationship and does not include accessing their own, family, employee or colleagues, or friends records for instance).
- → The Trust will apply the NHS Code of Practice on Confidentiality.
- → Employees are subject to standards of professional confidence (which will also apply to non-personal information in principle).

Protecting personal information: the Trust is required to employ appropriate technical and organisational measures to protect personal information. The Trust will apply such measures to non-personal information where appropriate. Security measures will be appropriate to the facility or process and include:

- → Keeping manual information secure and confidential;
- → Encryption on laptops, and other portable data devices;
- → Encryption on email messages containing personal or confidential information, and sending information to the right place;
- → Monitoring access to electronic health records by employees;
- → Deploying measures to resist or counter cyber-security threats or attacks.

Where it is necessary to destroy personal or confidential information in paper form this will be done by shredding. Computer disks will be disposed of by specialist

secure destruction by industry standard best practice method, and disposal catalogued.

The Trust will comply with Article 5 ***Principle* F of GDPR** Personal data shall be *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

3. Protect the Trust's information and communication technology infrastructure	
	*Integrity and confidentiality: The Trust has a duty to protect personal information however it is held, on paper or computer or other media (such as CCTV images, video or audio, for example). Personal information is subject to the Principles of the Data Protection Act 2018 and the Regulation. All of the Trust's information, information systems, equipment, and communication facilities must also be secure and protected to prevent theft, disruption to Trust business and care, and cyber-crime (hacking, theft or service disruption for instance).* *Physical measures such as locking doors, maintaining a 'clean desk', and looking after information or equipment in transit are also vital to ensure information security.*

The Trust has a duty to protect personal information, and compliance with **Article 5 principle F of the GDPR** is required by this section of the policy: *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

The Trust will deploy security measures, including physical, environmental, and knowledge processes, to protect personal information and organisational information. The Trust will secure assets with measures appropriate to the facility or process and include:

- → Encryption on all externally transmitted person identifiable information;
- → Encryption on laptops, PCs and other portable data devices;
- → PC or laptop desk locks where risk assessment identifies theft as a particular threat; and, business continuity measures where indicated;
- → The use of passwords on IT systems, access control, and other secure log-on and identification. Forced password change will apply via an expiry mechanism;
- → Authorising access to electronic health records based on the underlying principle of legitimate clinical relationship;
- → Firewall and virus protection;
- → Monitoring use of the internet and other systems to act against illicit activity:
- → Keypad access and locked doors, and;
- → Business continuity measures where indicated (uninterruptible power supplies, fail over infrastructure for key systems, and a server environment based on virtualisation and clustering, for instance).

Cyber-Security: The Trust will deploy measures to resist or counter cyber-security threats or attacks.

Cyber security relates to computers and computing, and is defined as the protection of systems, networks and data in cyberspace. Targeting Trust systems, services, or individual employees where illegitimate access, alteration or corruption of Trust systems, services or information is performed is potentially a criminal activity.

Employees must be vigilant to threat or attack. Appendix A provides a description of a number of cyber-security threats, which may include malware like:

→ Viruses, Worms, Spyware or Adware, or Trojans for example.

Attack types like:

→ Phishing, Pharming, Drive-by, MITM (Man in the middle attack), and Social engineering.

The Trust will conduct penetration testing to ensure the reliability and resilience of its information and communication technology infrastructure.

The Trust will provide information to employees about cyber-security and cyber threats and alert employees to such threat in information governance induction and training.

Offences: The Trust is required to comply with **the Freedom of Information Act (2000)**. It is an offence, under section 77 of the Freedom of Information Act, "to alter, deface, block, erase, destroy, or conceal any record once a request has been received." This applies both to information and personal information.

It is an offence under section 55 of **the Data Protection Act (1998)** to "knowingly or recklessly obtain or disclose personal data or procure the disclosure to another person."

The Computer Misuse Act (1990) has three main offences; unauthorised access to computer material; unauthorised access with intent to commit or facilitate commission of further offences; unauthorised modification of computer material, and had further offences added over the years. The Trust will consider taking action under this law if it is appropriate to do so.

4. Obtain information fairly and record efficiently

'Purpose limitation': The Trust is lawfully permitted to record and retain information about people, and use it for specific purposes. Information about patients (and cares and others) is used to support healthcare; employees for management and administration; suppliers for business purposes. The Trust is permitted only to collect and keep the information it requires.

The Trust must inform patients and other people (called data subjects in law) why we collect their information, what you are going to do with it and who you may share it with. We must make a record of this. We must be open, honest, and clear in doing so.

Stick to the facts, professional opinion and comment is permitted and record patient information in the Trust electronic health records system.

The Trust provides access to systems, internet and email. All are business systems provided for business use to support the Trust's patient care, management, governance, education, training, research and development activities.

The Trust uses electronic health records systems which must be used and kept up to date on a timely basis by practitioners. Patient information must be recorded as near to real time as practicable. This will include uploading any information which is temporarily noted or created on paper.

The Trust must comply with Article 5 principle B of the GDPR, which states *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

The Trust will complete a notification to the Information Commissioners Office annually detailing the purposes personal information is used for.

The Trust will apply Article 5 principle E of the GDPR, *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').*

All Trust records or information will be retained according to the preservation periods set out in the NHS Records Management Code of Practice, or where a statutory requirement exists.

5. Record information accurately and reliably

	*'Accuracy': The Trust uses electronic health records. Health records are a clinical tool, involved in virtually every consultation. They provide a clear and accurate picture of the care and treatment given to a patient - to serve that patient's clinical needs better. The record is for communication: practitioner to colleague, practitioner to or from other healthcare professionals, practitioner to themselves. Employees must ensure health records are clear, accurate, up to date, completed in a timely manner and well maintained. This will assist caring, safe and effective clinical practice and facilitate patient access to the record where requested.* *The Trust uses a variety of electronic record and information systems and all information in whatever form must be accurate and reliable.*

All employees are required to record high quality information, used appropriately, confidentially and securely. The information should be complete and as contemporaneous as possible. Information must be stored and retained in order that it can be accessed on an authorised basis.

The following standards will underpin the recording of all information in the Trust:

- **Validity**: All data items held on Trust computer systems must be valid. Where codes are used, these will comply with national standards or will map to national values. Computer systems will be programmed to only accept valid entries.
- **Completeness:** All mandatory data items within a data set should be completed. Use of default codes will only be used where appropriate, and not as a substitute for real data. Health records will be complete and contemporaneous.
- **Consistency:** Data items should be internally consistent.
- **Coverage:** Data will reflect all the work done by the Trust. Spot checks and comparisons between systems should be used to identify missing data.
- **Accuracy:** Data recorded on paper and on computer systems must be accurate and accurately reflect what actually happened, and all events should be recorded. In a legal case it is more difficult to defend an action or an omission if it is not evidenced in records. All reference tables will be updated regularly.
- **Timeliness**: recording of timely data is beneficial in terms of the treatment of a patient, and the operation of Trust services. Timely entry of information into Trust systems ensures information is available to all who need to use it. All data will be recorded to a deadline. Real time or near time recording of information should be the norm wherever practicable.

The fitness for purpose of personal information is legally regulated by the Data Protection Act and the GDPR, in particular the Trust must comply with **Article 5 principle D of the GDPR** *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').*

6. Use information effectively and legitimately	
	*'Storage limitation and Purpose limitation: Information must be available and fit for purpose, but we must also respect an individual's rights and record and use personal information appropriately, legally and accurately. The Trust must comply with the law and NHS governance.* *Effective and legitimate use of information will support providing a confidential service to patients, sharing information lawfully and appropriately and only accessing and using personal information you are entitled to.* *Employees have access to information and communication technology, systems discrete to the Trust and through the Internet which are for the effective performance of their duties. Using business facilities for business purposes will support caring, safe and effective practice. Not doing so may compromise patients, carers, employees and the Trust.* *The Trust must keep information for no longer than is necessary. Where a decision is made to create or retain personal information in an identifiable form this must be for no longer than is appropriate for the purpose. .*

Patient records: The Trust uses an electronic health record to record care and treatment provided to patients. The electronic health record can only be accessed by employees authorised to do so, using their own log on, and only records of patients the employee has a legitimate clinical relationship with may be accessed. The Trust monitors access to systems and records and may investigate and take disciplinary action where illegitimate access to systems or records occurs.

Paper records held by the Trust will remain accessible on an as required basis and will be stored securely. Records will be retained in accordance with NHS records management retention periods, disposed of in time and ultimately may be destroyed. Where records are disposed of by destruction this will be done securely and confidentially and destruction certified. Records must be securely and confidentially destroyed by shredding (or industry standard at the time) and not placed into ordinary waste for disposal.

Records maintenance, disposal and destruction: Records will be maintained by the Trust for periods set out in statute or guidance, and not for longer than is required. Where necessary personal data will be minimised. The Trust utilises electronic record systems and maintains electronic records where necessary. Where it is not possible to make a direct entry to the Electronic Health Record any written or other 'notes' must be promptly committed to electronic form and uploaded to the Electronic Health Record and be disposed of by destruction (shredding paper or deletion of notes).

The Trust will apply **Article 5 principle C and E of the GDPR**, to the collection or creation and retention of personal information. All Trust records or information will be retained according to the preservation periods set out in the NHS Records Management Code of Practice.

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Access to systems is not permitted for any illegal or immoral purpose. No employee is permitted to access, display or download offensive material, or transmit such material: to do so (on the face of it) is considered a serious breach of Trust policy and may result in dismissal, and could result in criminal action. The Trust is the arbiter on what constitutes offensive material, and what is or is not permissible system access and use.

The Trust Disciplinary Policy and Procedure (section 3.7) states that "the Trust reserves the right to suspend an employee where it is deemed to be in the interests of the employee, other employees or service users that the employee is withdrawn from the workplace, or where there is reason to believe that the capacity to conduct a thorough investigation may be compromised by the employee remaining at work". This will include the immediate withdrawal of an employee's access to the Trust's computer network, including services such as email, stored documents and access to electronic health records systems or any system or service if it is warranted.

Social media: Employees must not compromise patients or themselves personally or professionally, or the Trust, when engaged in any activity involving participation or use of any social networking media or other electronic, communication or broadcasting device.

Use of information for secondary purposes (non-direct care): The Trust will ensure that where patient information is used for purposes other than direct care the information will be used appropriately in a de-identified form (called pseudonymised), or the information will be totally anonymised. Such purposes are known as secondary use, where use of de-identified personal information is required and necessary for non-care purposes.

7. Share information appropriately and lawfully	
	*'Integrity and confidentiality.' Sharing information within the NHS, and other associated agencies, is imperative for ensuring good quality care to all our service users. However, such information sharing must be considered with respect for confidentiality.* *The Trust will always try to ensure that the patient has consented to the sharing of information, but it will share information without that consent where it is necessary to do so.*

When sending information employees are required to ensure that the information is in the right place, at the right time, and is the right information.

→ It is appropriate for employees to share patient information for direct care purposes;

→ It is appropriate to share patient information where it is not necessary for direct care purposes but there is a legal requirement to do this, or the risk is sufficiently severe to the individual or others to outweigh the duty of confidence to the patient.

- → Staff must deploy encryption on all externally transmitted person identifiable information (use of send secure email, NHS.Net, and authorised USB sticks procured from IT);
- → The Trust will require data processing agreements with third parties where use of personal information (defined in law as data processors) is required by a contract for a system or services;
- → The Trust will agree Information Sharing Protocols with other agencies or organisations, which set out the conditions for the exchange of patient information;
- → The Trust will comply with the requirement to submit mandatory 'minimum data sets' to NHS Digital, and contract data sets to commissioners of healthcare. Information which does not identify patients is used within the NHS for purposes that are not related to providing direct care. These may be statistical, managerial, or related to Public Health.
- → Measures will apply to sending data sets externally: peer checking is required, and sign-off by line management to ensure that only the data the recipient is entitled to receive is sent and the data to be sent is protected by secure and encrypted method.

The Trust will comply with *Article 44 GDPR, General principle for transfers: 1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. 2 All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. (Articles 45 to 50 apply in this sense)*

8. Support best practice

Best practice in information governance will ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to support delivery of the best possible care and treatment to patients.

Best practice is essential to ensure consistency in the way personal information is handled, maintain the confidence of patients and others and minimise the number of information incidents.

All employees are required to record high quality information, and use the information appropriately, confidentially and securely.

The Trust provides access to systems, internet and email. All are business systems provided for business use to support the Trust's patient care, management, governance, education, training, research and development activities.

The Trust uses assistive technology (video, audio, online communication, and telecommunication facilities) to support: the provision of patient care; the business

activities of the Trust; the provision of information; and, internal and external communication. This policy applies to any deployment of assistive technology, telehealth/telecare, home and community based clinical care and monitoring enabled by remote or mobile technology.

Information Governance training is mandatory and must be completed annually. The Trust provides face to face training at Trust Induction and provides a number of electronic platforms for completion of training on an annual basis thereafter. Targeted sessions for teams or groups of employees will also be provided as required.

4. Responsibilities

<table>
<tr><th>Management structure</th><th>Governance Structure</th></tr>
<tr><td>Board of Directors</td><td>Board of Directors</td></tr>
<tr><td>⇩</td><td>⇩</td></tr>
<tr><td>Accounting Officer
(Chief Executive)</td><td>Quality Committee | Data Protection Officer</td></tr>
<tr><td>⇩</td><td>⇩</td></tr>
<tr><td>Director of Finance | SIRO (Senior Information Risk Owner) | Caldicott Guardian</td><td>Well Led Committee</td></tr>
<tr><td>⇩ ⇩</td><td>⇩</td></tr>
<tr><td>Chief information Officer | Information Asset Owners | Line Managers</td><td>Information Management Group</td></tr>
<tr><td>⇩ ⇩</td><td>⇩</td></tr>
<tr><td>Head of Information Governance | Employees</td><td>Information Asset Owners</td></tr>
</table>

The **Chief Executive** is the Accounting Officer for the Trust, with overall responsibility for ensuring that the Trust applies legislation, policy and guidance in relation to Information Governance.

The Trust will have a **Senior Information Risk Owner (SIRO**), and supporting infrastructure. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of the Trust's Annual Governance with respect to this Policy.

The Trust's Board of Directors will appoint a **Caldicott Guardian**, whose role is to safeguard and govern uses made of patient information within the Trust, as well as data flows to other NHS and non-NHS organisations.

The Trust will appoint a Data Protection Officer: 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. The DPO is independent, an expert in data protection, adequately resourced, and report to the highest management level.

The role of **Information Security Manager** is incorporated within Informatics.

The **Director of Finance**, the **Chief Information Officer**, and the **Head of Information Governance** are responsible for co-ordinating compliance in the organisation and identifying key post-holders and providing guidance and advice on the application of Information Governance.

Managers and **Employees**: managers will ensure that this policy is made available to employees and will require all employees to confirm their familiarity with this policy. Managers will also check employee compliance with IG training requirements and ensure compliance with policy in the operation of their team. Qualified 'clinical' employees are also subject to their respective professional codes.

All **employees** are responsible for adherence to this policy within the organisation. Employees should ensure that any concerns about misuse of computers are reported to the Head of Information Governance. If employees suspect that any offences or breaches of policy are, can or might be committed, please seek advice from the Head of Information Governance, Caldicott Guardian, or Freedom to Speak Up Guardian.

The **Information Management Group** will keep adherence to this policy under review, this committee reports to the **Well-Led** Committee.

5 Training

Employees of the Trust will be required to attend Core Induction, including attendance at the Mandatory Information Governance training session.

Where Job Descriptions, KSF outlines, or conditions of employment require a minimum standard of proficiency relating to information governance education and training will be available to enable employees to achieve this.

The Trust will provide general information and facilitated information governance updates for employees.

Systems or applications involving personal identifiable data or corporate information will include as a condition of use training relating to information governance.

Information Governance training is mandatory for all employees, and must be done yearly. (Refer to the Trust mandatory training matrix).

6 Other relevant policies

This policy may apply and be read in conjunction with any Trust policies where the use of personal identifiable data or non-personal information is required.

7. Monitoring and Evaluation						
Criteria	**Measurable**	**Lead person/group**	**Frequency**	**Reported to**	**Monitored by**	**Frequency**
Systems in place to monitor the number of incidents and near misses reported involving employees, service users and others	Number of incidents and types reported	Head of Risk and Health and Safety/ Risk Management Team	Weekly	Weekly Review Meeting	Well-Led Committee	Quarterly
Compliance with policy	Data Security and Protection Toolkit	Head of Information Governance	Quarterly	Information Management Group	Well-Led Committee	Annually
Compliance with statute	Subject access and request for information response times	Head of Information Governance	Quarterly	Information Management Group	Well-Led Committee	Quarterly
Systems in place to monitor the number of complaints reported involving employees, service users and others	Number of complaints reported	Head of Complaints and PALS	Weekly	Weekly Review Meeting	Effectiveness Committee	Quarterly
Systems in place to monitor the quality	Health	Head of	Annually	Clinical Audit	Effectiveness	Annually

of information submitted to health records	Records Audit	Information Governance		Group	Committee	
Systems in place to monitor completion of an action plan created after completion of the health records audit	Health Records Audit Action Plan	Head of Information Governance	Annually	Clinical Audit Group	Effectiveness Committee	Annually
Systems in place to monitor the uptake of information governance training	Number of attendances	Head of Learning & Development	Quarterly	Information Management Group	Effectiveness Committee	Quarterly

Appendices/Procedure notes

Appendix A: Cyber Security

Types of malware

Cyber criminals operate remotely, in what is called 'automation at a distance', using numerous means of attack available, which broadly fall under the umbrella term of malware (malicious software). These include:

• Viruses - Aim: Gain access to, steal, modify and/or corrupt information and files from a targeted computer system.

Technique: A small piece of software program that can replicate itself and spread from one computer to another by attaching itself to another computer file.

• Worms - Aim: By exploiting weaknesses in operating systems, worms seek to damage networks and often deliver payloads which allow remote control of the infected computer.

Technique: Worms are self-replicating and do not require a program to attach themselves to. Worms continually look for vulnerabilities and report back to the worm author when weaknesses are discovered.

• Spyware/Adware - Aim: To take control of your computer and/or to collect personal information without your knowledge.

Technique: By opening attachments, clicking links or downloading infected software, spyware/adware is installed on your computer.

• Trojans - Aim: To create a 'backdoor' on your computer by which information can be stolen and damage caused.

Technique: A software program appears to perform one function (for example, virus removal) but actually acts as something else.

Attack angles:

There are also a number of attack vectors available to cyber criminals which allow them to infect computers with malware or to harvest stolen data:

• Phishing - An attempt to acquire users' information by masquerading as a legitimate entity. Examples include spoof emails and websites. See 'social engineering' below.

• Pharming - An attack to redirect a website's traffic to a different, fake website, where the individuals' information is then compromised. See 'social engineering' below.

• Drive-by - Opportunistic attacks against specific weaknesses within a system.

• MITM - 'Man in the middle attack' where a middleman impersonates each endpoint and is thus able to manipulate both victims.

• Social engineering - Exploiting the weakness of the individual by making them click malicious links, or by physically gaining access to a computer through deception. Pharming and phishing are examples of social engineering.

Appendix B: Internal Controls

The Trust will apply Internal Controls relating to Information Governance: comprising Procedures, Guidance, System Controls, and Assurance measures	
Procedures	Subject Access Request for personal information of employees and patients Request for Information under the Freedom of Information Act Privacy Notice: available on Trust Intranet and Internet and ''Health Record and Your Rights' available to Trust patients Care Record Guarantee Access procedures and user manual for Trust systems Incident Reporting Records management preservation periods and destruction schedule Clean desk environment Information Security Policy and associated guidance, procedures and user guides Business Continuity Procedures Information Sharing Protocols Privacy Impact Assessments Project Specifications to include information governance IT & IG Standard Operating Procedures (SOPs)
Guidance	Integrated Information Governance Guidance and Procedures (SOPs) Trust Code of Conduct (CORP13) NHS Records Management Code of Practice NHS Information Security Code of Practice Confidentiality: NHS Code of Practice Information Risk Management Code of Practice
System Controls	System User Manuals NHS Data Dictionary Mental Health Services Data Set Community Information Data Set Children and Young Peoples Data Set
Assurance	Information Governance Toolkit Performance Report Data Quality Reports/Audits Clinical Audits (as specified in the Trust Clinical Audit Plan) Care Quality Commission Essential Quality and Safety Standards

Appendix C: Internal Controls	

Art. 5 GDPR

Principles relating to processing of personal data

(1) Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').