Policy control document

This ensures good version control and effective policy management. It must be completed before a policy can be uploaded to the intranet.
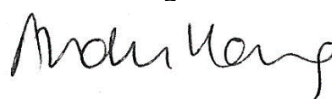
Policy Title	INTEGRATED INFORMATION GOVERNANCE POLICY
Policy Number	CORP 19
Author(s) (Name and Title/Role)	Mark Underwood, (Head of Information Governance) Laura Hamilton (Information Governance Manager)

Approval History	
Name of Committee	**Date**
Governance and Information Management	15/09/2010
Governance and Information Management	06/04/2011
Integrated Governance Committee	25/01/2012
Governance and Information Management	21/12/2012
Information Management Committee	22/11/2013
Information Management Committee	27/02/2014
Information Management Committee	15/10/2014
Information Management Group	15/01/2016
Effectiveness Committee	13/04/2017
Effectiveness Committee	18/01/2019
Quality Committee	08/07/2020
Committee which approved current version	**Date of approval for current version**
Quality Committee	**July/2022**

Date of next review (Month/Year)	**31st July 2024**

Chair of Approving Committee: Andrea Young

Signature:

Title: Non-Executive Director
Date: 07.09.2022

All policies are copy controlled. When a revision is issued previous versions will be withdrawn. An electronic copy of the current policy with be posted on the Trust Intranet.

Change control

Number of pages (excluding appendices): 14
Summary of Revisions: The policy has been extensively reviewed and revised. The policy review ensured that requirements of the data security and protection toolkit (DSPT) are met. The revisions also include recommendations from the ICO audit of November 2021.
Any change to code or merging with other policies
Consultation with: Information Management Group

Integrated Information Governance Policy

CORP19

Version 12
Date of approval 14th July 2022

Contents

1. Purpose of policy (aims and objectives)

The purpose of this policy is to set out the Trust requirements for effective information governance as this is essential to delivering our core values of Caring, Safe and Excellent. The policy provides a consistent way for employees and those working in or on behalf of Oxford Health NHS Foundation Trust (contractors, temporary workers, secondees, substantive, volunteers etc.) to deal with the many different information handling requirements within their roles. This policy also contains procedural elements to assist staff in the performance of their duties. Information Governance is concerned with the right information being in the right place at the right time and accessed appropriately.

The aim of these integrated policy is to ensure:

- The Trust complies with the law and the NHS regulatory framework.
- Personal information is accurately recorded and used appropriately.

Integrated Information Governance Policy **CORP 19**

- Information is available only to the people who need access.
- Information is shared appropriately.
- All information and information assets are secure, and confidence assured.

By achieving the aims of these integrated policies the Trust will be able to demonstrate compliance with legislation and meet information governance obligations.

Objectives: –

1. To obtain a minimum of satisfactory status in the annual Data Security and Protection Toolkit audit.
2. To achieve 95% compliance with Integrated Information Governance Mandatory Training across the Trust.
3. To comply with all legislative and NHS Information Governance requirements.
4. To ensure staff are aware of Information Governance requirements within the Trust.

2. Outline of 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.

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.

This policy includes procedures and is supported by guidance, system controls, assurance, awareness raising and formal training.

Confidentiality and Data Protection

The use of confidential information by Oxford Health is essential for the effective provision of healthcare and supporting functions. Generally the Trust processes personal information under what is referred to as the Trust 'Public Task'. Maintaining confidentiality should not be confused with keeping secrets.

- Information about people (personal information) can only be used where there is a lawful basis.
- 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 accessing their own, family, employee or colleagues, or friends records for instance is strictly forbidden).

- The legitimate relationship principle also applies to using personal information about colleagues or other people.
- Employees are subject to standards of professional conduct with respect to the use of information (this will also apply to non-personal information).
- The Trust recognises that to provide safe patient care or protect others it may be necessary to break a confidence. Staff should involve their line manager/supervisor for assistance prior to making decisions around this.

There are offences under sections 170 - 173 of **the Data Protection Act (2018)** related to unlawfully obtaining and using personal data for which the individuals responsible can be prosecuted.

Subject Access Request (SAR)

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 people in accordance with the UK GDPR and Data Protection Act (2018). Requests can be made verbally, in writing or by third parties.

A subject access request can apply to any personal information held by the Trust regardless of the media on which the information is recorded for example, chat, email, patient or staff record, Microsoft documents or spreadsheets.

Staff should be aware that if they receive a request for information held by the Trust about an individual, they must send the request to subject.access@oxfordhealth.nhs.uk immediately. This will enable the Trust to meet the obligation of responding to SAR requests without undue delay and within one month at the latest of the request being received by a member of the Trust.

Freedom of Information (FOI)

The Trust is required to comply with the Freedom of Information Act (2000) that provides public access to information held by public authorities.

FOI applies to all recorded information held by Oxford Health in any recorded format.

It is an offence, under section 77 of the Freedom of Information Act, "to alter, deface, block, erase, destroy, or conceal any record once an FOI request has been received." This applies both to information and personal information.

The Trust will meet its obligation to publish certain information about their activities on the Trust Internet site.

Staff should be aware that if they receive a request for information from members of the public, they must send the request to foiarfi@oxfordhealth.nhs.uk without undue delay. This will enable the Trust to meet the obligation of responding to FOI requests within 20 working days.

Information Governance processes FOI requests but will contact staff in the Trust to collate and provide information requested.

Information Security & Protection

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. Staff are also individually responsible for protecting personal information and applying the following measures. Security measures include:

- Keeping manual information secure and confidential.
- Encryption on laptops, PCs, and other portable data devices.
- Encryption on email messages and all externally transmitted person identifiable or confidential information.
- Sending information to the right place by double checking addresses.
- Deploying measures to resist or counter cyber-security threats or attacks.
- Destroy personal or confidential information in paper form by shredding.
- Computer disks or other media should be disposed of by specialist secure destruction by industry standard best practice method, and disposal catalogued.
- Multi Factor Authentication will be utilised in systems where technically feasible.
- 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.
- Access to electronic health records based on the legitimate clinical relationship and role-based access control.
- Access to information shall be restricted to users who have an authorised organisational need to access the information as approved by the relevant Information Asset Owner (Usually Head of Service) or nominated deputy.
- Firewall and virus protection.
- Utilising cloud enabled applications in accordance with ICO guidelines and Principles on Cloud computing.
- Monitoring use of the internet and other systems to act against illicit activity.
- Monitoring access to electronic health records by employees.
- Keypad access and locked doors, PC or laptop desk locks.
- 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).
- Deploy measures to resist or counter cyber-security threats or attacks. (Further cyber security information is available in Appendix A).
- Conducting penetration testing to ensure the reliability and resilience of its information and communication technology infrastructure.
- Providing information to employees about cyber-security and cyber threats and alert employees to such threat in information governance induction and training.
- All information assets will be identified and assigned an Information Asset Owner (IAO)

Password Standards

Integrated Information Governance Policy **CORP 19**

- Change your passwords regularly
- Do not share your passwords with anyone.
- Ensure passwords are a mix of characters, numbers, and special characters

Encryption and Secure Email

- The Trust deploys encrypted email that is automatically applied to nhs.net and .gov email addresses. For all other external email address including nhs.uk, staff should always use [Send Secure] at the beginning of the email subject line**.**
- Staff should only store personal data on encrypted memory sticks devices provided by the IT Service.

Device Management

- Staff should not attempt to connect personal devices to Trust services without IM&T Department approval (e.g. email, wireless etc.).
- Staff must not install software on Trust equipment without IM&T Department approval.
- Staff must not move/relocate IT equipment (including telephones) to different desks/offices without IM&T Department approval.
- Staff should not access Office 365 applications on non-trust devices.

Procurement

For purchases of new technologies, systems, services and applications (Apps) staff must follow the Trust Procurement Policy and where appropriate ensure that a cyber assessment, Security and Infrastructure Assessment, an IG Assessment and if necessary and Data Protection Impact Assessment (DPIA) are completed as part of the due diligence process.

Appropriate Use of IT Systems

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 disciplinary proceedings including 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 reserves the right to immediately withdraw a system users 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: Staff must refer to the Trust Code of Conduct with reference to social media.

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.

Recording Events

Integrated Information Governance Policy **CORP 19**

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 for the recording where practicable.

Where MS Teams is used to record an event consideration should be given to the nature of the event and the privacy and awareness of the participants.

Consideration needs to be given to recording events where personal data is being referred to or participants are named and identified. Access to such recordings should be strictly controlled and staff should be aware that the recording could constitute personal information and be requested under data protection.

The Trust operates CCTV systems that are managed by Estates and Facilities for the purposes of crime prevention, public safety, and health and safety. Please refer to the Trust CCTV policy for further information on the Risk Management and Health and Safety Policy section of the intranet.

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.

The Trust applies National Data Opt Out and staff should consult the National Data Opt Out guidance on the IG Intranet.

Data Protection by Design and Default
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, including cyber security assessment, IM&T security and infrastructure assessment and information governance assessment. A data processor agreement will be required where personal information is being processed by a third party.

Information Incident Management
The Information Commissioners Office (ICO) defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data breaches should be reported within 72 hours of discovery. The Head of Information Governance or nominated deputy will consider if the incident meets the criteria for reporting to the ICO.

If staff discover a data breach they should:

Integrated Information Governance Policy **CORP 19**

1. Immediately take steps to secure the data e.g. retrieve it or ask for it to be deleted, amend the access group.

2. Raise the incident in Ulysses without delay and speak to the line manager.

3. Assess the risk of the data breach and if appropriate/necessary, notify and apologise to the person/people the data has been breached as soon as possible.

Records Management, Retention and Data Quality

The Trust creates a broad variety of information, documents and records on multiple media which are 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 by practitioners. Patient information must be recorded on a timely basis and as near to real time as practicable. This will include uploading any information which is temporarily noted or created on paper.

All employees are required to record high quality information. Trust information should be 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 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.

Patient records

Integrated Information Governance Policy **CORP 19**

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).

Data Retention

Records will be retained in accordance with the NHSx Records Management Code of Practice 2021. Where records are destroyed this will be done securely, confidentially and destruction certified. Records must be securely and confidentially destroyed by industry standard and not placed into ordinary waste for disposal.

Information Sharing

- It is appropriate for employees to share personal information when there is a lawful basis for doing so.

- There may be occasions where it is necessary to share confidential information for health or safety or other legal purposes (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. In such circumstances staff should discuss the matter with their line manager/supervisor and the Caldicott Management Principles should be applied notwithstanding that it is still necessary to comply with the law (Caldicott Principle 6). The information sharing should be recorded in the clinical record.

- 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/Agreements with other agencies or organisations, which set out the conditions for the exchange of information.

- The Trust are required 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 minimum data the recipient is entitled to receive is sent and the data to be sent is protected by secure and encrypted method.

- Decisions to share personal information will be recorded. A disclosure related to an individual's care should be recorded in the clinical record. Statutory disclosures such as subject access requests, personal information required for the investigation or detection of crime, or the prosecution or apprehension of offenders (police or other statutory requirements) should be administered and recorded by the Health Records team.

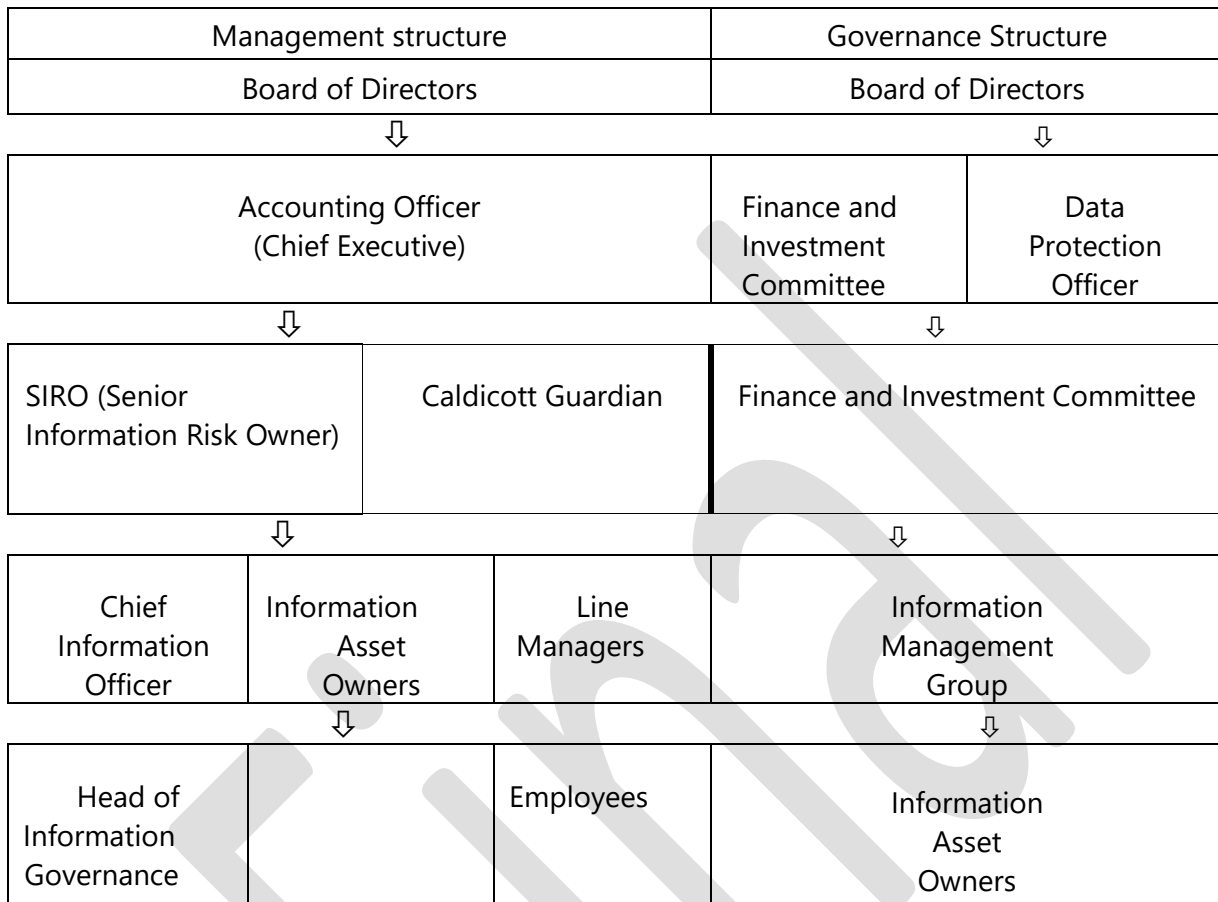### 3. Summary of actions to implement policy (*Guidance in Appendix C*)

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.

8. Encourage best practice.

9. Staff must attend mandatory IG training annually, and managers must monitor the IG training compliance for their team.

4. 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.

- **UK General Data Protection Regulation (2021)**

- **Privacy and Electronic Communications Regulations (2022)**

- **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.

- **Public Records Acts 1958 and 1967**: sets out what 'government' information should be permanently preserved and made available for public access.

- **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.

- **NHS Records Management Code of Practice 2021:** 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.

- **Data Security and Protection Toolkit:** NHS Digital online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data standards

- **Care Quality Commission Essential Quality and Safety Standards: CQC Regulation**
  The Healthcare regulators standards for governance.

5. Key responsibilities

Management structure			Governance Structure	
Board of Directors			Board of Directors	
⇩			⇩	
Accounting Officer (Chief Executive)			Finance and Investment Committee	Data Protection Officer
⇩			⇩	
SIRO (Senior Information Risk Owner)	Caldicott Guardian		Finance and Investment Committee	
⇩			⇩	
Chief Information Officer	Information Asset Owners	Line Managers	Information Management Group	
⇩			⇩	
Head of Information Governance		Employees	Information Asset Owners	

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

Senior Information Risk Owner (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.

Caldicott Guardian: whose role is to safeguard and govern the uses made of patient information within the Trust, as well as data flows to other NHS and non-NHS organisations.

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.

Information Security Manager: has IM&T responsibilities for the security and protection of systems and infrastructure.

Integrated Information Governance Policy **CORP 19**

Managers: are responsible for ensuring 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 take appropriate action to ensure compliance by their team.

Employees: are responsible for adherence to this policy within the organisation and for ensuring they complete their IG training annually. 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. Qualified 'clinical' employees are also subject to their respective professional codes.

The **Information Management Group** will keep adherence to this policy under review, this committee reports to the **Finance and Investment Committee.**

6. Training required to implement policy

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

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).

7. Monitoring and evaluation

There should be clear criteria by which to monitor implementation of the policy and evaluate its effectiveness and appropriateness. This is usually expressed as a table.

Measure	Lead (Name and Title)	Group/ Committee that measures will be reported to by lead	Frequency of Reporting
Mandatory IG Training	Information Asset Owner	Information Management Group	Quarterly
DSPT	Head of Information Governance	Information Management Group	Annually
ICO Audit	Head of Information Governance	Information Management Group	As request by ICO
Escalation Report	Chair of IMG	Finance and Investment Committee	Quarterly

Integrated Information Governance Policy **CORP 19**

8. Appendices

This Policy is supported by guidance and reference materials that are published on the Information Governance pages of the Trust Intranet.

Appendix A: Cyber Security

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.
- → 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.

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 acts as something else.

Attack angles:

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

Integrated Information Governance Policy **CORP 19**

- *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: UK GDPR Article 5 Principles

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) of the applied GDPR, 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) of the applied GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation the applied GDPR 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,

Integrated Information Governance Policy **CORP 19**

using appropriate technical or organisational measures ('integrity and confidentiality'). or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Appendix C - Guidance on Summary of Action to Implement Policy

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. Several 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 UK 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 identifying 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

Integrated Information Governance Policy **CORP 19**

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 UK GDPR, supported by good information governance practice, will also ensure compliance with *Chapter 3 of the UK 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.

The Trust will apply **Article 5 principle C and E of the UK 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) of the applied GDPR subject to implementation of the appropriate technical and organisational measures required by the applied GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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.

The Trust will comply with Article 5 ***Principle*** **F of UK GDPR** Personal data shall be *processed in a manner that ensures appropriate security of the personal data, including protection against*

Integrated Information Governance Policy **CORP 19**

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 cybercrime (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 UK 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').*

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 must comply with Article 5 principle B of the UK 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),*

Integrated Information Governance Policy **CORP 19**

of the applied GDPR 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 UK 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) of the applied GDPR subject to implementation of the appropriate technical and organisational measures required by the applied GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation').*

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.

The fitness for purpose of personal information is legally regulated by the Data Protection Act and the UK GDPR, in particular the Trust must comply with **Article 5 principle D of the UK 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

Integrated Information Governance Policy **CORP 19**

'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.

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.

The Trust will comply with *Article 44 UK GDPR, General principle for transfers: 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 the applied GDPR, the conditions laid down in this Chapter of the applied GDPR 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. All provisions in this Chapter of the applied GDPR shall be applied in order to ensure that the level of protection of natural persons guaranteed by the applied GDPR is not undermined. (Articles 45 to 50 apply in this sense)*

8. Support best practice

Integrated Information Governance Policy **CORP 19**

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.

Integrated Information Governance Policy **CORP 19**

Equality Analysis (EqA) Screening Form

Name of Policy/Procedure/Practice/Project/Programme/Plan: Integrated Information Governance Policy

Equality Analysis (formerly known as Equality Impact Assessment) is a thorough and systematic analysis of a policy, practice or procedure to ensure it is not unlawfully discriminating against any group with a protected characteristic.

An equality analysis is:
- A tool for delivering equality
- A keyway of demonstrating that you have given 'due regard' to equality considerations as prescribed by the public sector equality duties in the Equality Act 2010
- Part of good policy and service delivery governance
- A positive activity which should identify improvements

Please use this EqA Screening Form to examine and identify any differential impact for any of the protected characteristics and to prompt mitigation of the adverse/negative impact before it is approved by the relevant committee.

This Screening Form can be used at the beginning of the equality analysis process to gather initial feedback, thoughts and ideas, or at quarterly intervals to monitor implementation of a project/programme, or at the end on completion to assess impact or outcome.

If this Screening Form reveals any adverse/negative impact for any of the protected characteristics listed below, you may need to complete a full Equality Analysis (Form EqA1). For further details (including a copy of the EqA1 Form), please see Equality Analysis Procedure and Guidance which can be found on the Polices Site.

For advice, information and guidance, please contact the Head of Inclusion at: EqualityandInclusion@oxfordhealth.nhs.uk

Protected Characteristic	Positive Impact	Neutral Impact	Negative Impact	Comments/Evidence
	√	√	√	
Age	✓			Legislative Compliance
Disability	✓			Legislative Compliance
Sex/Gender	✓			Legislative Compliance
Race/Ethnicity	✓			Legislative Compliance
All Faiths & None	✓			Legislative Compliance
Sexual Orientation	✓			Legislative Compliance
Transgender	✓			Legislative Compliance
Pregnancy & Maternity	✓			Legislative Compliance
Marriage & Civil Partnership	✓			Legislative Compliance

Completed by:-
Name: **Mark Underwood**
Title: **Head of Information Governance**
Date: **17 June 2022**