Arthington Medical Centre

5 Moor Road, Hunslet, Leeds, LS10 2JJ
0113 385 2180

CONFIDENTIALITY AND DATA PROTECTION POLICY

Review and Amendment Log / Control Sheet

Author:	West Yorkshire ICB Senior Information Governance Officer
Date Approved:	April 2023
Approved by:	Mena Suri
Version:	1.0
Review Date:	April 2025

Version History

Version no.	Date	Author	Status	Circulation
1.0	April 2023	Senior IG Officer	Approved	All Practice Staff

Executive Summary

This policy aims to clarify the principles that govern the use of personal information and to ensure that practices are understood and adhered to and applies to all employees of the Practice, staff who work for, or on behalf, of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice, (referred to as staff / /employees from this point on).

All Staff have a common law duty of confidentiality to patients and a duty to support professional ethical standards of confidentiality. This applies to **all types of information** whether held on paper or electronically and whether passed in written form or orally. All person identifiable information should be accessed, stored and disposed of securely.

This policy aims to ensure that:

- there are nominated persons responsible for data protection
- everyone that handles personal / confidential information:
  a) understand their responsibility for following good data protection practice
  b) is appropriately trained to do so
- anyone who receives or wants to make an enquiry about accessing personal information knows what to do.

The Practice is committed to the delivery of a first-class confidential service. This means ensuring that all person identifiable information is processed fairly, lawfully and as transparently as possible so that our patients and staff:

- Understand the reasons for processing personal information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way we handle information held about them

We may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used, e.g. on a computer or on paper, this personal information must be dealt with appropriately to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) The lawful and proper treatment of personal information is extremely important to the success of our business and in order to maintain the confidence of our service users and employees.

The failure of the Practice to comply with data protection legislation could potentially result in a subsequent investigation by the Information Commissioner's Office, with the possibility of being fined up to £17.5 million higher standard or 4% of the total annual worldwide turnover in the preceding financial year whichever is higher or £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year whichever is higher.

Equality Statement

This policy applies to all employees, Managing Partnership members and members of Arthington Medical Centre irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION

Arthington Medical Centre recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The Practice also recognise the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which they process, store, share and dispose of information.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified. It is essential that all staff and contractors of the Practice are fully aware of their personal responsibilities for information which they may come into contact with.

2. AIMS

The aim of the policy is to ensure that all staff understand their obligations regarding any information they come into contact within the course of their work and to provide assurance that the Practice have in place the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively.

The Practice will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the UK GDPR and the DPA 2018 and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Protection and Security Toolkit (DSPT).

This policy supports the Practice in their role as providers of health services and will assist in the safe sharing of information with partners and agencies.

3. SCOPE

This policy must be followed by all staff who work for or on behalf of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, Managing Partnership members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

- All aspects of information within the organisation, including (but not limited to):
- Patient/Client/Service User information
- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of, the organisation.
- Practice information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including (but not limited to):

- Organisation, adoption, or alteration of information
- Retrieval, consultation, storage/retention, or use of information
- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons.
- Alignment, combination/linkage, blocking, erasing or destruction of information

Confidentiality and data protection within the practice is the responsibility of the data controller (owner/partners).

The Practice recognise the changes introduced to information management as a result of the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key information governance roles and bodies that the Practice needs to have in place as part of its Information Governance Framework, these are:

- Data Protection Officer (DPO)
- Managing Partnership
- Governance, Performance and Risk Committee
- Caldicott Guardian
- Information Asset Owner/Administrator
- Heads of Service/department
- All employees

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

Please refer to the glossary contained in this policy.

6. ENSURING INFORMATION IS SECURE AND CONFIDENTIAL

6.1 General Principles

- The Practice regard all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework will be achieved, monitored, and maintained.
- The Practice regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Practice will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality, Privacy and Electronic Communications Regulations, the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, regarding responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective, and affordable confidentiality and data protection controls are in place.
- Where any disclosure of personal data is made there a must be a legal basis for doing so.

6.2 Using and Disclosing Confidential Patient Information for Direct Healthcare

Consent to share personal information for direct care is usually based on implied consent, which may also cover administrative purposes where the individual has been informed or it is otherwise within their reasonable expectations. When information sharing is needed for direct healthcare patients should still be informed about:

- The use and disclosure of their healthcare information and records.
- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.
- The potential use of their records for the clinical governance and audit of the care they have received.
- Through a privacy notice outlining what information will be shared, the purpose of this, who the data will be shared with, how long data will be retained, the rights of the data subject and what security measures are in place to protect confidentiality.
- If not for direct care then explicit consent or some other legal basis must be present to enable sharing.

Under the UK General Data Protection Regulation and Data Protection Act 2018 when processing personal data in the delivery of direct care and for associated administrative purposes, the following conditions of lawful processing that are available to all publicly funded health and social care organisations in the delivery of their functions will apply:

- UK GDPR Article 6 (1) (e) for the performance of a task carried out in the public interest or in the exercise of official authority.
- UK GDPR Article 9 (2) (h) medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

6.3 Using and Disclosing Confidential Staff Information

Processing of personal data where the information sharing is needed for direct communications related to their role, salary payment and pension arrangements, is lawful. Staff should be made aware that disclosures may

need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of freedom of information requested where the public interest in disclosure is deemed to override confidentiality considerations.

Using staff information for other purposes must be subject to explicit consent being granted unless another legal basis permits this.

6.4 Using and Disclosing Corporate and Business Information

All staff should consider all information which they encounter through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes.

6.5 Information Security

Rules and guidance on information security are set out in The Information Security Policy (which sets rules, guidance and good practice on ensuring security of information in the workplace, on areas such as portable devices, email, paper and electronic systems) and the Records Management and Retention polices which includes sections on transfer of, storage and archival of records.

6.6 Sharing Confidential Information Without Consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. to safeguard a child) or a court order must be in place. In deciding on any disclosure certain considerations and steps need to be taken:

- Discuss the request with the appropriate personnel such as the Caldicott Guardian and/or IG Lead.
- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- Follow any locally agreed Information Sharing Protocols and national guidance.

Requests may be received by other agencies which are related to law enforcement such as:

- The Police or another enforcement agency where the appropriate request form (in line with the Access to Records Procedure) needs to be submitted from the law enforcement agency for the Practice to consider the request.
- The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Staff should also take into account the seventh Caldicott principle and Information Governance Alliance guidance if there is a clear legal basis to share.

6.7 Confidentiality and Conversations

Where during your work you have conversations relating to confidential matters which may involve discussing (or disclosing information about) individuals such as patients or staff members you must ensure:

- Check individuals contact preferences
- That such discussions take place where they cannot be overheard.
- That for telephone calls the rule is you do not give out confidential information over the phone - unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak with another team member on the phone who is based at another location).
- Where you receive a request over the telephone for confidential information ask the caller to put the request in writing so details can be verified.
- That you do not discuss confidential work matters in public places or at social occasions.
- Where an answer phone is used ensure that recorded conversations on cannot be overheard or otherwise inappropriately accessed.

6.8 Records Management

The Practice have a Records Management/retention schedule which should be followed for all aspects of record creation, sharing, storage, retention, and destruction of records.

6.9 Access to Records

Individuals have a right to request access to their records in line with the UK GDPR / DPA 2018 by making a Subject Access Request (SAR). All staff should familiarise themselves with the Practice access to records procedure which should be followed for all requests for personal data. This procedure

also gives guidance in relation to requests for the records of deceased people under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

Access to corporate information and records will be in accordance with Practice Freedom of Information Act and Environmental Information Regulations Policy.

6.10 Information Sharing

The Practice will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Code of Conduct and in accordance with the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015.

Any local Information Sharing Protocols that the Practice have signed up to need to be always followed, unless they conflict with law or statute.

6.11 Information Confidentiality Breaches

All actual, potential or suspected incidents involving breaches of confidentiality or cyber-related incidents must be reported on the Datix system following the Practice Incident Reporting procedure.

All incidents involving patient data should be reported to the Caldicott Guardian, who should consider whether serious breaches of confidentiality, or those involving large numbers of individuals, need to be reported to the Information Commissioner via the Data Security and Protection Toolkit incident reporting tool in accordance with the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Reportable breaches should be determined and presented within 72 hours of being identified.

What should be reported?

Misuses of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. The following list gives some examples of breaches of this policy which should be reported:

- Sharing of passwords and/or smartcards.

- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential personal information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification, and you have concerns that it is not in accordance with the data protection principles and NHS Code of Confidentiality.
- Sending data in a way that breaches confidentiality.
- Leaving confidential information lying around in a public area e.g., photocopier.
- Theft or loss of patient-identifiable information.
- Disposal of confidential information in a way that breaches confidentiality i.e., disposing of patient records and or content of in an ordinary wastepaper bin
- Processing identifiable information without an appropriate Information Asset and associated data flows being identified and recorded in the organisations register.

6.12 Data Protection Impact Assessment

All new projects, processes and systems (including software and hardware), which are introduced that include person identifiable data, must meet data protection by design and confidentiality requirements. To enable the Practice to identify and minimise any data protection risks, a Data Protection Impact Assessment (DPIA) must be undertaken. A DPIA will:

- Identify privacy risks to individuals
- Protect the Practice reputation
- Ensure person identifiable data is being processed safely
- Foresee problems and negotiate solutions
- Identify all Information Assets and corresponding data flows
- Document the legal basis for processing.

The Practice's procedure for DPIAs should be followed.

6.13 Objections and Opt-Outs

Where patient identifiable information is being processed for purposes other than direct care, there is an obligation to respect opt outs that have already been presented.

The National Data Opt Out programme enables patients to opt out from their personal health care data being used for research or planning purposes.

This programme is explained within the ICB's privacy notice and further information is available from the National data opt-out - NHS Digital website.

6.14 Individuals' Rights

The GDPR provides individuals with key rights to control and influence how data about them is used. These general rights are captured below although it is important to note that they are not absolute (they change depending on the legal basis for processing being used) – advice must be sought from the IG team if staff are unclear what action is required.

The right to be informed	The Practice must provide information about how it uses information about individuals. Staff must be aware of the privacy notice(s) in place to support this.
The right to access	Individuals may ask for access or copies of the information held about them by the Practice. Staff should be aware of the Subject Access Request and Access to Health Records procedure, which supports this.
The right to rectification	Individuals can challenge the accuracy of personal data held about them and ask for it to be corrected or deleted if there are factual errors or omissions. Staff must consider such corrections.
The right to erasure	Individuals can request their data be deleted and in some (not relating to health or social care purposes) circumstances, the Practice will need to respect this. Staff should seek advice from the IG team if they receive such a request.
The right to restrict processing	Individuals can limit the way the Practice uses personal data if they are concerned about the accuracy of the data or how it is being used. Staff should seek advice from the IG team if they receive such a request.
The right to data portability	Individuals have the right to obtain their personal data in an accessible and machine-readable format. Staff should seek advice from the IG team if they receive such a request.
The right to object	Individuals may object to the processing of their personal data. Staff should seek advice from the IG team if they receive such a request.
Rights in relation to automated decision making	Individuals can ask that automated decisions and profiling without any human involvement do not happen. Staff should seek advice from the IG team if they receive such a request.

Further information can be found on the ICO Website.

7. CONFIDENTIALITY GUIDANCE AND LEGISLATION

For personal and confidential Information held by the Practice there will be appropriate measures to ensure confidentiality and security, underpinning the principles of Caldicott, NHS Digital Guidance, ICO and professional Codes of Practice, legislation and common law.

7.1 UK General Data Protection Regulations

The UK GDPR requires that data controllers ensure personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- 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 not be incompatible with the initial purposes.
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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 subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals
- 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.

It is important to note that the Regulation specifies that:

- organisations are accountable for how they handle personal data and need to develop and maintain adequate policies, procedures, processes and systems to fulfil this role.
- data processors can be held liable for breaches
- all actual information breaches must be reported via the IG Toolkit (to the ICO) within 72 hours of becoming known

- the penalty for breach of the Regulations is £17.5 million higher standard or 4% of the total annual worldwide turnover in the preceding financial year whichever is higher or £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year whichever is higher.
- organisations must employ the privacy by design approach to activities involving personal data. A Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- fair processing notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU
- the consent model for processing personal data is to be further defined (see Caldicott 3 report and corresponding consultation and direction from the Department of Health)
- as part of the implementation of the Regulations, a register of data controllers, will no longer be maintained by the ICO
- data subjects have the new right to erasure, data portability, review of automated decision making and profiling, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within 30 days and provided free of charge (unless a request is “manifestly unfounded or excessive”)
- organisations must keep a record of processing activities
- appointment of a Data Protection Officer

The Data Protection Act 2018 includes the national derogations of the UK GDPR and the implementation of Law Enforcement Directive (EU) 2016/680:

- Specific exceptions from the UK GDPR (primarily in schedules 2-4)
- The processing of personal data for law enforcement
- It defines which organisations are considered Public Authorities
- Process of reporting and potential consequences of data breaches
- The processing of personal data relating to children under the age of 13 years and the ability to seek the consent of children aged 13 years or older for some information services
- Role and powers of ICO and provision to charge fees
- Conditions for processing - listed
- Allowances for complaints and compensation, which can now include financial loss, distress and other adverse effects.

- Establishes new criminal offences: “knowingly or recklessly to re-identify information that is de-identified personal data”, data theft, unlawful obtaining of personal data and alteration of personal data in a way to prevent it being disclosed.

7.2 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

7.3 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further. This applies to all types of information whether held on paper or electronically and whether passed in written form or orally and must not normally be disclosed without the individual’s consent.

There are three circumstances where disclosure of confidential information is lawful:

- where the individual to whom the information relates has consented.
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest.
- where there is a legal duty to do so, for example a court order.

Any decision to disclose without consent must be fully documented and agreed by the Caldicott Guardian.

The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

7.4 Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure. She was asked to conduct a further review and a new

report: ‘Information to share or not to share’ was published in March 2013 and was updated and expanded in December 2020. The recommendations of this report have been largely accepted by the government and a revised set of Caldicott Principles were published:

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised, and documented with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is necessary
Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. The need to keep patients and service users informed, and to ensure that their expectations are considered and met when their confidential information is used.

This is ensuring that there are no surprises for the public. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is use, and what choices they have about this.

The Caldicott Guardian also has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. A detailed description of the Caldicott Function is given in the Information Governance Strategy.

In 2014, the post of National Data Guardian was established, with the role of helping to make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

7.5 Information Commissioner's Office Codes of Practice

The Practice processes data that is covered in the following Codes of Practice published by the Information Commissioner's Office (ICO):

- Data sharing
- Subject access
- Closed Circuit Television
- Privacy Notices
- Employment Practices
- Anonymisation
- Personal Information Online
- Privacy Impact Assessments

7.6 NHS Digital

NHS Digital is responsible for facilitating the management and sharing of data across the NHS to support both operational and other functions such as planning, research and assessments. NHS Digital has produced a Code of Practice: A Guide to Confidentiality in Health and Social Care - NHS Digital

7.7 The NHS and Social Care Record Guarantees for England

The NHS and Social Care Record Guarantees for England sets out the rules that govern how individual care information is used in the NHS and in Social Care. It also sets out what control the individual can have over this.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly with regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

7.8 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health and Social Care in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable. Regulations under the Act support the sharing and use of information for defined commissioning activities and support NHS structure, subject to safeguards.

7.9 Health and Social Care Act 2012

The Health and Social Care Act 2012 provides NHS Digital with a legal basis to process identifiable data and on behalf of other NHS organisations. The Act proves the authority to operate Data Service for Commissioners (DSfC) and Data Service for Commissioners Regional Offices (DSCROs).

7.10 Health and Social Care (Safety and Quality) Act 2015

The Health and Social Care (Safety and Quality) Act 2015 sets the expectation that information will be shared between health and social care in the interests of individuals. Individuals are able to override such sharing if they have an objection. The Act is seen as key to enabling the Caldicott principle of there being a duty to share between those health and social care professionals involved in the direct care of patients if it is in the best interests of those individuals.

7.11 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not

directly involved in or to obtain or view information about friends and relatives.

- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.

- Modify data or programs held on computer without authorisation.

7.12 Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which are relevant to Data Protection and confidentiality which may have an effect on disclosure and use of information (see list below). This is not an exhaustive list. Where you need any further guidance regarding any of the legislation or guidance listed - you can contact the organisation's Caldicott Guardian or the Information Governance lead (see section 11 Advice and Guidance).

- Abortion Regulations 1991
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 2018)
- Access to Medical Records Act 1988
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Data Retention and Investigatory Powers Act 2014
- Digital Economy Act 2017
- Communications Act 2003
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Fertilisation and Embryology Act 1990
- Human Rights Act 1998
- Medical Act 1983
- Mental Capacity Act 2005
- NHS Digital. "FAQs on legal access to personal confidential data." Accessed 16 September 2016. Available from http://digital.nhs.uk/article/3638/Personal-data-access-FAQs.
- NHS Sexually transmitted disease regulations 2000

- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004

All staff are bound by the codes of conduct produced by any professional regulatory body, by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

8. TRAINING

8.1 Mandatory Training

The Data Security Protection Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance in accordance with the IG Training Strategy.

Line managers must actively ensure that all staff undertake and complete the annual mandatory information governance training.

8.2 Specialist Training

Additional training may be provided in specialist areas such as data protection. The need for additional training should be identified with reference to the IG Training Strategy.

9. IMPLEMENTATION AND DISSEMINATION

Following ratification this policy will be disseminated to staff via an appropriate method e.g. the Practice intranet and communication through in-house staff briefings.

This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

10. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Data Security Protection Toolkit (DSPT), will be undertaken each year. This includes confidentiality and data protection. Incidents are reported and all serious information governance issues are escalated appropriately.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the https://cfa.nhs.uk/reportfraud or telephoning 08000 28 40 60.

11. ADVICE AND GUIDANCE

Advice and guidance on any matters stemming from the Policy can be obtained by contacting the West Yorkshire Information Governance Team: wyicb-leeds.dpo@nhs.net.

12. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

This policy should be read in conjunction with:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Mobile Working Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and social media Policy
- Email Policy

And their associated procedures (including but not limited to):

- Subject Access Request (Access to Health Records) Procedure
- Information Sharing Protocol

- Freedom of Information Procedures
- Privacy Impact Assessment Procedure and supporting documents
- Safe Transfer Guidelines and Procedure

This policy should also be read in conjunction with the Information Governance Handbook which provides guidance for staff on information governance compliance.

13. GLOSSARY

Term Used	Definition of word or phrase
Bulk transfer of person identifiable or sensitive data	Used to describe information relating to 21 or more individuals.
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Consent	The consent of the 'data subject' means any freely given, specific, informed, and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
Corporate Information	All categories of corporate information should be regarded as confidential in the first instance although they may be releasable through the Freedom of Information Act regime, including via the Publication Scheme. This includes (but is not limited to): • Governing Body and committee meeting papers and minutes • Tendering and contracting information • Financial information Project and planning information
Data Controller	Data Controller means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor	Processor means a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller.

Term Used	Definition of word or phrase
Data Protection Officer (DPO)	The DPO is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance which includes conducting assurance audits.
Data Subject	An identified or identifiable 'living individual' whose personal data is processed by a controller or processor. Otherwise known within data protection legislation as a 'natural person'.
Declaration	Declaration is the point at which the document (i.e. the record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Document	The International Standards Organisation (ISO) standard 5127:2017 now states 'recorded information shall be treated as a unit in a documentation process regardless of its physical form or characteristics'.
Electronic document	Information recorded in a manner that requires computer or another electronic device to display, interpret and process it. This includes documents (whether text, graphics or spreadsheets) generated by software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in Electronic Data Interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.
Encryption	The process of transforming information (referred to as plain text) using an algorithm (called 'cipher') to make it unreadable to anyone except those possessing special knowledge, usually referred to as a 'key'.

Term Used	Definition of word or phrase
File Plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet the records management needs.
Folder	A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable). Folders are allocated into a class.
Health Record	Information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual.
Information Asset Owners (IAOs)	Are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several information assets.
Information Asset Register	Is a list of information assets owned by the Practice.
Information Assets	Are operating systems, infrastructure, business applications, off the shelf products, services, user- developed applications, records and information.
Information lifecycle management	Information lifecycle management is the policies, processes, practices, services, and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Records Management policies and procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage, records audit etc.

Term Used	Definition of word or phrase
Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Mobile Computing	Covers the use of portable computing devices, such as laptops, mobile phones, tablet computers, memory sticks or equivalent mobile computing equipment.
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record, or folder.
Network	A system that connects two or more computing devices for transmitting and sharing information. Inclusive of all components processing data at organisations point of entry and excludes any end user devices connecting to a switch, hub or wireless access point or any systems monitoring network devices.
Network File Server	Is computer hardware with large storage capacity which is held in a highly secure area.

Term Used	Definition of word or phrase
Personal Data	Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, including (but not limited to): • Name • Date of Birth • Post Code • Address • National Insurance Number • Photographs, digital images etc. • NHS or Hospital/Practice Number • Location data Personal data that has been pseudonymised can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.
Processing	Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each identifiable patient data item. It enables NHS organisations to undertake secondary usage of patient data in a legal, safe and secure manner.

Term Used	Definition of word or phrase
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (the ISO standard, ISO 15489-1:2016 Information and documentation - records management).
Records Management	The process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.
Responsible User	Individual members of staff who personally adhere to the Practice's IT Security Policy (incorporating Network Security) and make use of the computer facilities provided to them by the Practice in an appropriate and responsible fashion.
Safe Haven	A term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the Practice whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles.

Term Used	Definition of word or phrase
Senior Information Risk Owner (SIRO)	The SIRO is a senior officer of the Practice. The SIRO acts as an advocate for information risk for the Practice and leads and implements the information risk assessment programme.
Special Category Data	Special Category Data (or sensitive personal data) are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Subject Access Right	Entitles the data subject to have access to and information about the personal data that a controller has concerning them. Also known as the Right of Access.
Users (end users)	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much or the material which constitutes the record. Since records systems tend to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.