Information Governance Policy

Document History

Document Reference:	01
Document Purpose:	This policy sets out the expectations for Bromsgrove Primary Care Network employees are required to manage information in line with legislation and national guidance.
Date Approved:	September 2023
Version Number:	2.0
Status:	Approved
Next Revision Due:	September 2024
Developed by:	Umar Sabat, Data Protection Officer
Policy Sponsor:	Primary Care Network Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Bromsgrove Primary Care Network.
Associated Documents:	Data Protection Impact Assessment Policy, DSP Toolkit submission, Confidentiality Policy, Privacy Policy

1. Introduction

1.1 Information governance is the framework of law and best practice regulates that the manner in which information, whether internally or externally generated and in any format or media type is managed i.e., obtained, handled, used and disclosed). It is a complex and rapidly developing area and one of utmost importance since information lies at the heart of the organisation and underpins everything it does.

1.2 Information Governance is an umbrella term for a collection of distinct but overlapping disciplines. Reference to information governance in this policy shall mean reference to the following areas as well:

- Access to information (Freedom of Information Act 2000, Data Protection Act 2018, General Data Protection Regulations)
- Confidentiality and data protection
- Information security assurance
- Records and document management

1.3 The organisations records are its corporate memory, providing evidence of actions and decisions and representing a vital assert to support daily functions and operations. Records support policy formation and managerial decision-making protect the interests of the organisation and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.4 The organisations Board has adopted this policy and is committed to on-going improvement of its information governance functions to ensure that it continues to use information safely, securely and for the purposes it is intended for.

1.5 This policy is the responsibility of the Information Governance and Data Protection Officer who is supported closely by the Primary Care Network Manager.

2. Purpose

2.1 The organisation is committed to ensuring that its information is managed to the highest standards and in accordance with all relevant legislative requirements, including the Data Protection Act 2018, GDPR and the Freedom of Information Act 2000; best practice guidance organisations such as the Information Commissioners Office (www.ico.gov.uk) and NHS Digital (www.digital.nhs.uk).

2.2 The purpose of this policy is to ensure that all types of information held by the organisation, whether that is corporate, patient, or personnel information, are kept safe, secure and managed appropriately. This includes ensuring that:

- Records are available when needed.
- Records can be accessed.
- Records can be interpreted.
- Records can be trusted.

- Records can be maintained through time.
- Records are secure.
- Records are retained and disposed of appropriately.
- Staff are trained.
- Patients are informed.

2.3 To this end the organisation commits itself to:

a) **Information Governance Management –** establishing and maintaining robust operational and management accountability structures as well as assigning appropriate resources and expertise to ensure information governance issues are dealt with appropriately.

b) **Systems and Processes** – implementing information systems and processes to enable the efficient and secure storage and retrieval of information and the management of information risk.

c) **Training and Awareness** – implementing a system of training and awareness that is role based, assessed and capable of equipping staff with the skills and knowledge necessary to carry out their responsibilities.

d) **Audit** – Monitoring staff compliance with the information governance framework through regular audits

3. Scope

3.1 This policy sets out the organisations approach to ensuring it has a robust information governance framework to manage its information assets, in particular, operational and management structures, roles, responsibilities, systems, policies, procedures and audit controls that the organisation has established to ensure such issues are appropriately addressed throughout the organisation.

3.2 This policy will be available to all staff employed Bromsgrove PCN including Consultants who are carrying out work on behalf of Bromsgrove PCN. All staff are responsible for remaining up to date with and adhering to this policy.

4. Duties

4.1 The Information Governance Lead, has overall responsibility for information governance in the organisation.

4.2 The Board of Directors is responsible for ensuring that the information governance function is addressed at a strategic level. They will ensure there is an adequate level of resources and expertise to deal with the range of issues that arise across the information governance function.

4.4 The Primary Care Network Manager is responsible for information governance at an operational level and is accountable to the Board of Directors. Some members of the management team are also nominated Information Asset Owners.

4.5 The nominated Board member is the Senior Information Risk Owner (SIRO). The Senior Information Risk Owner (SIRO) acts as champion for information risk on behalf of the Board. They advise the Board of the performance of the Information Governance function of the organisation, ensure it is given appropriate resources and commitment, and is appropriately communicated to all staff. They lead on information security assurance; ensure that all information risks are dealt with in line with the Risk Assessment Policy & Procedure and that all information incidents follow the organisation's Incident Reporting & Duty of Candour Policy.

4.6 The Information team will meet regularly to monitor progress against the Information Governance agenda. The Board has granted the Primary Care Network Manager to make decisions relating to the Information Governance agenda and to approve new policies, amendments to policies and related documents.

4.7 The Information Governance Lead has day-to-day operational responsibility for all aspects of Information Governance which includes answering detailed questions from people using our services about the use of their information.

4.8 All staff are reminded of the need to adhere to the Caldicott Principles as set out in Appendix A. Alongside the Data Protection Act Principles, these represent best practice for using and sharing confidential or identifiable information and should be applied whenever a disclosure or use of information is being considered.

4.9 Information Asset Owners (IAOs) and Information Asset Assistants (IAAs) are responsible for maintaining the confidentiality, integrity, and availability of all information their Information Asset holds. A Business Continuity Plan is needed for all information assets should a threat occur. Each Information asset will be recorded on the Information Asset Register which will be regularly maintained and updated with the relevant IAO to ensure its accuracy.

4.10 Line Managers are responsible for operational staff and monitor their compliance with the information governance agenda.

4.11 Staff are individually responsible for ensuring that they comply with the information governance framework and will ensure that all work programmes acknowledge the requirements of the framework.

5. Training and Awareness

5.1 Staff will be provided with information governance training relevant to their role at induction and are required to complete further mandatory training on an annual basis.

5.2 Staff who will have more contact with information or with roles defined in this policy will be required to complete relevant modules on E-Learning for Health provided by Health Education England.

5.3 Staff may also be required to complete additional training where appropriate.

5.4 Contractors are also required to complete basic IG training.

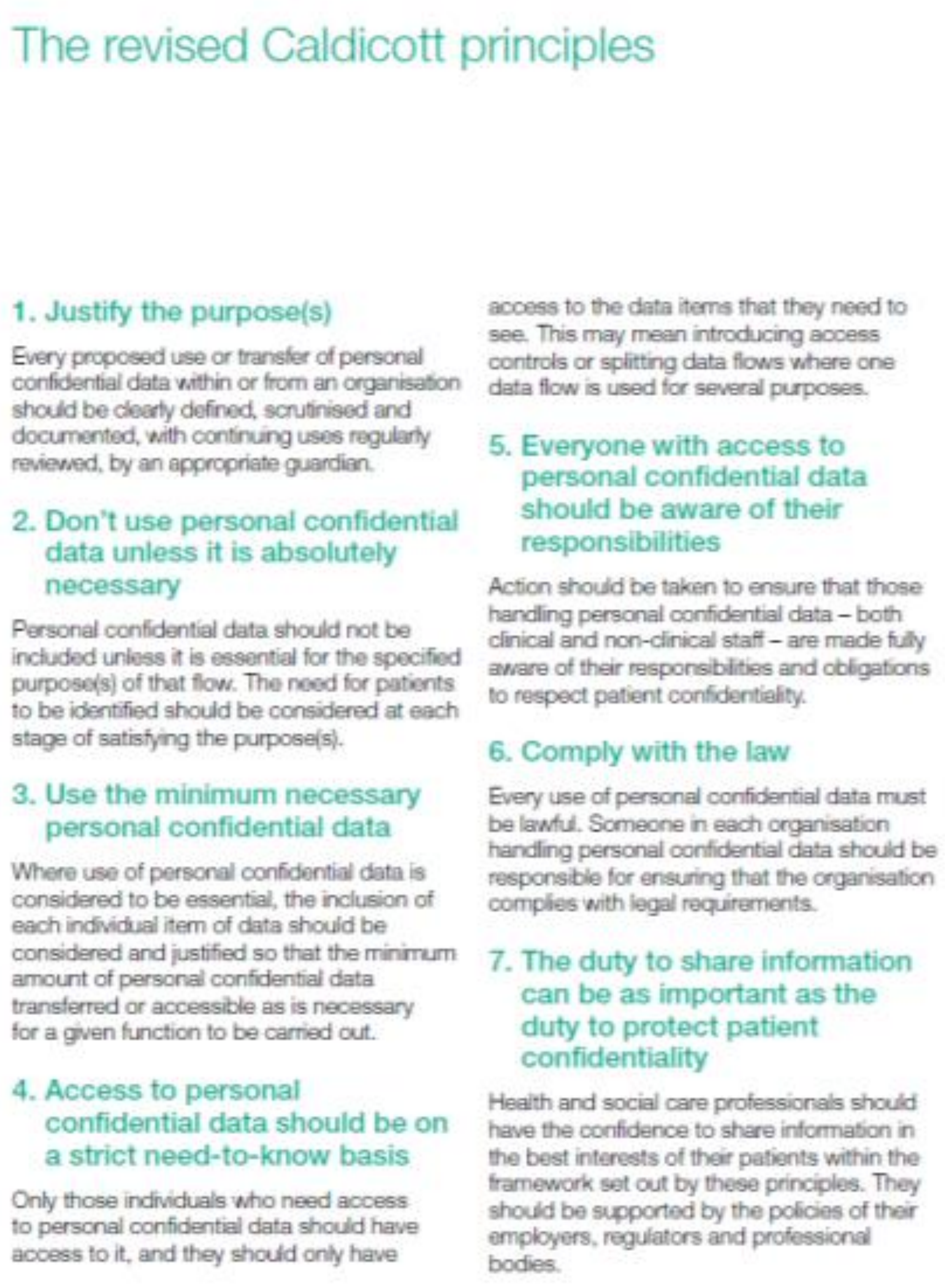
6. Legislation and Key Documents

- The Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice
- The Information Commissioners Office: Data Protection Handbook

7. Equality Impact Assessment

An initial equality impact assessment has been carried out and there are no differential impacts on any of the protected characteristics. Therefore, a full equality impact assessment is not required.

Appendix A – Caldicott Principles



The revised Caldicott principles

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 absolutely necessary

Personal confidential data 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 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. 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 framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.