KINGSWINFORD

Medical Practice

Data Protection and Confidentiality Policy

Change Control

Version	To	Change	Date
1	2	Numbering removed	12 July 2019
1	2	Changes to style and headings	12 July 2019
1	2	New Headings and Content table	12 July 2019
1	2	Removal of reference to Data Protection Act 1998	12 July 2019
1	2	Removal of reference to IG toolkit	12 July 2019
1	2	Updated links to NHS guidance	12 July 2019
2	3	Safeguarding guidance link	1 April 2020
3	4	Reviewed and updated	6 April 2021
4	5	Reviewed and updated	3 January 2022
5	6	Reviewed	4 January 2023
6	6.1	Reviewed no changes	31 March 2024
6.1	6.2	Updated for DSP Toolkit 2024/25	11 June 2025
6.2	6.3	Updated for DSP Toolkit 2025/26	7 April 2026

Document History

Document Reference:	IG01
Document Purpose:	This policy sets out the practice Kingswinford Medical Practice expect from all staff, including those working on behalf of the practice, when complying with Data Protection legislation within the practice.
Date Approved:	7 April 2026
Version Number:	6.3
Status:	FINAL
Next Revision Due:	April 2027
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Victoria Evans – Practice Business Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the practice or volunteering with the practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2025/26
DS&P Toolkit Standard	

Data Protection and Confidentiality Policy

Review dates and details of changes made during the review

This is a new policy developed to support Kingswinford Medical Practice compliance with the NHS Data Security and Protections Toolkit.

Key words

Information Governance (IG), confidentiality, security, data protection, IG Toolkit, SIRO, Caldicott Guardian, Privacy, DS&P Toolkit, DUAA

Summary

This document provides a policy statement on the use and management of information in the practice and describes the arrangements for providing assurance to the practice management team that IG compliance standards are defined and met and IG incidents appropriately managed.

Introduction

The Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) 2016 and Data Use and Access Act 2025 (DUAA) impose obligations on the use of all personal data held by the practice whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the practice. This has implications for every part of the practice. The practice also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, NHS Digital and the NHS Information Governance Alliance the specific requirements NHS Digital Data Security and Protections Assurance Toolkit and guidance issued by professional bodies.

The practice and its employees are bound by a legal duty of confidentiality to all patients which can only be set aside to meet an overriding public interest, legal obligation, or similar duty. The DPA and UK GDPR apply to all staff, contractors and volunteers working for the practice. The practice is a Data Controller, as defined in Article 3 (7) of the UK GDPR and Section 1 of the DPA, and is obliged to ensure that all the Data Protection requirements are implemented, the requirements of Article 5 (1) of the UK GDPR and be able to demonstrate compliance with those requirements Article 5(2).

This policy sets out how the practice meets its legal obligations and requirements under confidentiality, Data Protection and information security standards. The chief requirements outlined in this policy are based upon the DPA/UK GDPR, which is the central piece of legislation covering security and confidentiality of personal information.

Policy aims

This Data Protection and Confidentiality Policy aims to ensure that the practice meets its legal obligations and NHS requirements concerning confidentiality and information security standards.

The requirements within the policy are primarily based upon the DPA and UK GDPR, being key pieces of legislation covering security and confidentiality of personal information.

Policy scope

This policy covers all forms of information held by the practice, including but not limited to:

- Information about members of the public
- Non-practice employees on practice premises
- Staff and personnel information
- Organisational, business and operational information

This policy applies to all practice employees and third parties responsible for the delivery of contracted NHS services on behalf of the practice.

Definitions

Information Governance (IG) - IG is the organisational practice of managing information from its creation to final disposal in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that practice information is managed securely, compliant with legislation and available for access by both staff and external parties, including the public and regulators.

Data Security and Protections Toolkit **(DS&P)** - the assessment toolkits are supported by both NHS Digital and NHS England and are a self-assessment tool for practices which incorporates a knowledge base and guidance of all aspects of IG. The IGT/DS&P is updated annually to reflect new NHS guidance, legislation and NHS codes of practice.

Senior Information Risk Owner (SIRO) - the SIRO takes ownership of the practice's Information Risk Policy and acts as an advocate for information risk on behalf of the practice who is also the SIRO.

Caldicott Guardian **-** the practice's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is Dr Louise Butler.

Data controller - means the natural or legal person, public authority, the practice, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing are determined by Union or Member State law. The controller or the specific criteria for its nomination may be provided for by Union or Member State law, Article 4(7) UK GDPR.

Principles of DPC policy

To meet the vision for managing DPC standards there are three key interlinked aims to the policy which will ensure the delivery of an effective policy framework:

- **Legal compliance -** the practice aims to meet and exceed all compliance requirements relating to DPC. The practice will undertake or commission annual assessments and audits of its compliance with legal requirements through the Appropriate IG Toolkit and demonstrating compliance to all relevant healthcare standards, the policy will also demonstrate that the practice has adopted the accountability for demonstrating compliance with the UK GDPR as required by Article 5(2)
- **Information security -** the practice will promote effective confidentiality and security practice to its staff through an Information Security Management Systems (ISMS) which includes policies, procedures and training. The practice has established and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security
- **Openness -** non-confidential information on the practice and its services should be available to the public through a variety of media. The practice will undertake or commission annual assessments and audits of its policies and arrangements for openness through the IG Toolkit

The practice has developed the Data Protection and Confidentiality Policy to enable the delivery of these three key aims for this policy.

Roles and responsibilities

Practice management team

The practice management team has overall accountability for the practice's ability to meet the policy requirements. The management team is responsible for:

- Receiving, considering and approving regular reports and briefings
- Signing off the practice's privacy strategy and annual IG and DS&P toolkit returns
- On behalf of the management team, the Information Governance Steering Group (IGSG) is responsible for ensuring adequate arrangements are in place

Executive lead

The Senior Partner has overall responsibility for IG in the practice. As accountable officer she is responsible for the management of IG within the practice and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The practice has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Caldicott Guardian

The practice Caldicott Guardian has management team level responsibilities for the practice's Caldicott function and enables a direct reporting line to the practice management team and the appropriate governance committee. The Caldicott Guardian is responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to IG and will require an IG lead to liaise directly with the Caldicott Guardian.

Senior Information Risk Officer

The SIRO has management team level responsibilities and takes overall ownership of the practice's IG processes and provides written advice to the senior partner on the content of the practice's annual governance statement in regard to information risk.

Information Governance Steering Group

The IGSG is responsible on behalf of the practice for:

- Developing, implementing and maintaining an ISMS and associated policies, an annual work programme to provide assurance to the practice that effective arrangements are in place
- Agreeing IG relevant reports and recommendations and timely preparation of the annual IG assessment for practice management team sign off
- Promote and embed IG into the organisational culture.

IG Lead – Practice Business Manager

The nominated IG Lead is the Practice Business Manager. Emma Drew, Dr C Field and Dr L Butler are also IG Leads. The IG Leads have responsibility for project managing the overall co-ordination, publicising and monitoring of the practice IG framework. The practice IG Leads have specific responsibility for the development of this policy, producing performance monitoring reports and producing IG toolkit central returns on behalf of the practice.

Data Protection Officer – PCIG Consulting Limited

Paul Couldrey of PCIG Consulting Limited will act as the Data Protection Officer (DPO) for the practice. This role is key to ensuring that practices comply and can demonstrate that they comply with the UK GDPR.

Practice employees & staff working on behalf of the practice

All practice employees, whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All employees are required to undertake regular practice mandatory training in IG to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance. Misuse of or a failure to properly safeguard information may be regarded as a disciplinary offence. It is important that staff a have an understanding of the legal framework and good practice guidance issued by their own professional bodies for sharing information to assist with multi-agency safeguarding enquiries, case discussions, serious case reviews (SCRs), multi-agency learning reviews (MALRs), domestic homicide reviews (DHRs), safeguarding adults reviews (SARs), multi-agency risk assessment conference (MARAC), multi-agency public protection arrangements (MAPPA), vulnerable adult risk management (VARM) meetings (county only), etc.

Safeguarding

Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers.

Available from:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

In general, safeguarding teams should be able to quote their legal powers to exempt their requests from UK GDPR non-disclosure issue, ask for the request formally quoting their legal powers if they have a legal power consent is not required.

For the purposes of safeguarding children and vulnerable adults, the following Article 6 and 9 conditions may apply:

> *6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…' and*
>
> *9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..'*

In particular *social protection law.*

As information relating to criminal convictions and offences are not special categories data, practices will need to reference the Article 10 provisions of the DPA18 as a basis for processing of such data for safeguarding purposes.

To meet the requirement in Article 9(2)(b) that the processing is necessary for the purposes of carrying out the obligations of the controller or data subject in the field of social protection law, the provisions of the Children Acts 1989 and 2004 and the Care Act 2014 are relevant.

The Children Act 1989 (CA) establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm.

The CA also requires local authorities '*to safeguard and promote the welfare of children within their area who are in need'* and to request help from specified authorities including NHS Trusts and Foundation Trusts, NHS England and CCGs. These are required by the CA to comply *'…with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions.'* Under the Children Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being.

The Care Act 2014 sets out a clear legal framework for how local authorities and other parts of the system should protect adults at risk of abuse or neglect. Local authorities have a duty to make enquiries where an adult is experiencing or is at risk of experiencing abuse or neglect and has duties to collaborate with partners generally and in specific cases.

It remains the responsibility of practices and the professionals they employ to ensure that they have a basis for processing that meets common law requirements and the requirements of the UK GDPR and for public bodies that they are acting within their powers.

Policy statements

When practice staff manage any business information then she/he is required to comply with the requirements of the procedures and requirements. This policy requires all staff to manage information to the highest standards to ensure compliance with appropriate standards, to secure all practice information and to promote appropriate information access.

The practice fully endorses the six principles set out in the UK GDPR 2016. The practice and all staff who process personal information must ensure these principles are followed. In summary these state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- 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')
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
- 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')

Furthermore, the practice is committed to implementing the eight Caldicott principles.

The Caldicott principles

The Caldicott Principles (as updated December 2020) require all practices having access to confidential information to exercise good practice when dealing with confidential information for non-healthcare purposes:

- Justify the purpose(s) of using confidential information
- Only use it when absolutely necessary

- Use the minimum that is required
- Access should be on a strict need-to-know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform Patients and service users about how their confidential information is used

The Caldicott Guardian must approve any use of patient identifiable data for non-healthcare purposes.

Any breach of the Data Protection legislation with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with practice policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

Subject Access (SAR/DSAR)

There is a recognised procedure (the patient access to medical records policy & proxy access 2021) by which personal data is disclosed either to the data subject or to their representative.

Any request must be completed within a maximum of one month from date or receipt, from 25th May 2018 under UK GDPR rules. There will be no fee charged for SAR.

Confidentiality

The 'Confidentiality: NHS Code of Practice' has been published by NHS England. The consultation included patients, carers and citizens, the NHS, other health care providers, professional bodies and regulators.

This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

Patient confidentiality

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent, effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

On first contact with the practice, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

In the event a person lacks capacity to consent to information being shared, staff should check if a person is authorised by a Lasting Power of Attorney (health and welfare) or been appointed by the court of protection to make that decision. The document must be seen. This person can consent on their behalf but must act in the person's best interest. If they have not, then no one can consent on behalf of that person. A professional in the care team must assess if it is in the best interest of the person to share the information. The person's wishes and feeling, although not determinative, should be the starting point in this assessment.

Staff confidentiality

All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications must be conducted in a confidential manner.

Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager or GP Partner. Staff must not process any personal information in contravention of the UK GDPR 2016 or DPA 2018.

Any breaches of these requirements will potentially be regarded as serious misconduct and, as such, may result in disciplinary action.

All staff have a confidentiality clause in their contract of employment. The practice has an approved Data Protection and Confidentiality clause in all contracts with third party contractors and suppliers who process personal information.

Education and training requirements

The practice is committed to the provision of IG training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery.

The practice has a mandatory training programme which includes maintaining awareness of IG, data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:

- Personal responsibilities
- Confidentiality of personal information
- Relevant IG policies and procedures
- General good practice guidelines covering security and confidentiality
- Records management

All staff will be required to complete annual IG training, (including data protection and confidentiality training), commensurate with their duties and responsibilities. All new starters will be given IG training as part of the practice mandatory induction process.

Process for monitoring compliance

The IG lead will establish a performance management framework, reported through the IGSG on a six monthly basis.

Equality impact assessment

The practice recognises the diversity of the local community it serves. Our aim, therefore, is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

Legal liability

The practice will generally assume vicarious liability for the acts of its staff, including those on honorary contract. However, it is incumbent on staff to ensure that they:

- Have undergone any suitable training identified as necessary under the terms of this policy or otherwise
- Have been fully authorised by their line manager to undertake the activity
- Fully comply with the terms of any relevant practice policies and/or procedures at all times
- Only depart from any relevant practice guidelines providing always that such departure is confined to the specific needs of individual circumstances. In healthcare delivery such departure shall only be undertaken where, in the judgement of the responsible clinician it is fully appropriate and justifiable, such decision to be fully recorded in the patient's notes
- Staff contracts of employment are produced and monitored by the practice. All contracts of employment include a data protection and general confidentiality clause as part of controls to enhance privacy and information governance. Agency and contract staff are subject to the same rules

Supporting references, evidence base and related policies

The SIRO will direct the IG leads to take actions as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies in particular:

- NHS Records Management Code of Practice Part 2
- NHS IGA UK GDPR Guidance
- Information Security Management: NHS Code of Practice

There are a number of policies and procedures within the practice that should be read in conjunction with this document for a complete understanding of how the practice is organised and the strategies in place to fulfil its obligations.

The key documents are listed below:

- Patient Access to Medical Records Policy and Proxy Access 2018
- Practice responsibilities document
- Records Management and Retention Policy
- Data Breach Reporting Policy

Due regard

This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation, to advance equality of opportunity and foster good relations.

Review and monitoring

The Practice Business Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.

This policy will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.