

Data Protection, Confidentiality and information Security Policy and Procedures

Policy Statement

Edinburgh GP medical practice processes personal data relating to employees and patients and is therefore required by law to comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), the Data (Use and Access) Act 2025 (DUAA), and other applicable data protection and confidentiality legislation. These requirements protect the privacy of individuals and ensure that personal data is processed lawfully, fairly, transparently and securely.

The practice is committed to ensuring that it complies with applicable data protection legislation and applies ethical and professional principles to all aspects of its work to protect the interests of employees and patients and maintain the confidentiality, integrity and security of personal data held in any form by the practice.

The practice follows the seven data protection principles under the UK GDPR. In summary, these state that personal data shall be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification for no longer than is necessary;
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- processed in accordance with the principle of accountability, with the practice able to demonstrate compliance with the UK GDPR.

The practice will also ensure that any restricted international transfers of personal data are undertaken in accordance with the requirements of UK data protection legislation.

We also recognise the rights of individuals under the UK GDPR, subject to applicable legal conditions and exemptions:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.

- The right to restrict processing.
- The right to data portability, where applicable.
- The right to object.
- Rights in relation to automated decision-making and profiling, where applicable.

The practice has developed a Privacy Notice for Patients and a Privacy Notice for Staff.

The practice also maintains a separate Data Protection Complaints Policy setting out the procedure for making, acknowledging, investigating and responding to data protection complaints.

Lawful Basis

The practice does not rely upon a single lawful basis for all processing of personal data. The lawful basis used will depend upon the purpose and circumstances of the processing and will be identified and documented before processing takes place.

The practice may rely upon one or more of the lawful bases under Article 6 of the UK GDPR, including, where appropriate:

- processing necessary for the performance of a contract;
- processing necessary for compliance with a legal obligation;
- processing necessary to protect vital interests;
- processing necessary for the purposes of legitimate interests, where applicable and where the interests, rights and freedoms of the individual do not override those interests; and
- consent, where consent is the appropriate lawful basis.

Where the practice processes special category data, including health information, an Article 6 lawful basis must be identified together with an additional condition under Article 9 of the UK GDPR.

For the provision of healthcare and treatment, the practice will generally rely upon Article 9(2)(h) of the UK GDPR, where the relevant requirements are met. The associated condition in UK law is set out in Schedule 1, Part 1, Condition 2 of the Data Protection Act 2018. This condition covers processing necessary for:

- preventive or occupational medicine;
- the assessment of an employee's working capacity;
- medical diagnosis;
- the provision of health or social care or treatment; and
- the management of health or social care systems or services.

The practice will ensure that the appropriate Article 6 lawful basis and Article 9 condition are identified for the relevant processing activity. These do not necessarily have to be the same or directly linked.

The practice will not rely on patient consent as the lawful basis for all healthcare processing. Where personal information is shared for the provision of healthcare, the practice will consider the applicable lawful basis, the duty of confidentiality, professional requirements and whether patient consent or another form of authorisation is required in the particular circumstances.

The practice will document its lawful bases and purposes for processing in accordance with its accountability obligations and will include relevant information within its Privacy Notices.

Responsibilities

This Data Protection, Confidentiality and Information Security Policy applies to all practice employees, clinicians and any others who have legitimate rights to access and use the practice's information systems.

Compliance with UK data protection legislation and this policy is the responsibility of all practice employees and everyone who has access to practice records.

A breach of this policy, whether deliberate or through negligence, may lead to disciplinary action and, where appropriate, referral to the relevant professional or regulatory body. Serious breaches of data protection legislation may also result in enforcement action, financial penalties or criminal offences where applicable under legislation.

The following table lists key responsibilities among the medical team.

Team Member	Responsibility
Lead Doctor & Data Protection Officer, Dr David Richardson AND Kirsty Wales, Practice Manager	Overall responsibility for the Data Protection, Confidentiality and Information Security Policy; oversight of data protection compliance; dealing with Subject Access Requests and other data protection rights requests; oversight of data protection complaints in accordance with the separate Data Protection Complaints Policy; staff training regarding data protection and confidentiality; oversight of data breaches and information security incidents.
David Richardson	Data controller responsibilities as applicable to the processing undertaken by the practice.
Alanna Merrie	Data controller responsibilities as applicable to the processing undertaken by the practice.
Shona Williamson	Data controller responsibilities as applicable to the processing undertaken by the practice.
Stephen Miller	Data controller responsibilities as applicable to the processing undertaken by the practice.
James Robertson	Data controller responsibilities as applicable to the processing undertaken by the practice.
Rebecca Chessbrough	Data controller responsibilities as applicable to the processing undertaken by the practice.
All staff	Compliance with UK data protection legislation and this Data Protection, Confidentiality and Information Security Policy.

Where the practice acts as the data controller, the practice is responsible for determining the purposes and means of processing personal data. Individual clinicians will comply with the practice's data protection, confidentiality and information governance arrangements and their professional obligations.

If you have any questions or comments about processing personal data or this policy, please contact the Practice Manager/Data Protection Lead.

Definition of Personal Data Covered Under the UK GDPR

The UK GDPR applies to personal data, which is information relating to an identified or identifiable living individual. This includes an individual's name, address, telephone number, email address, online identifiers, employment records and other information which can identify an individual directly or indirectly.

There is also 'special category' information which requires additional protection, including information concerning health, racial or ethnic origin, religious or philosophical beliefs, genetic or biometric data where used for identification, trade union membership, political opinions, and information concerning a person's sex life or sexual orientation.

The UK GDPR applies to personal data processed electronically and to certain manual records where information forms part of, or is intended to form part of, a structured filing system.

To provide effective care for patients and provide healthcare services, the practice processes personal data of patients. Personal data means practically any information about, or correspondence relating to, an identifiable individual. It includes both facts and professional opinions, including:

- personal information and contact details, including the patient's name, address and date of birth;
- medical, social and medical histories (e.g. past or current medical conditions, current medication, the name of the patient's NHS GP and relevant special needs);
- results of the GP consultation/assessment;
- information about appointments;
- any treatments and their costs;
- any proposed care, including advice given to the patient and referrals the patient might need;
- any concerns that the patient or medical team might have;
- details of the patient's consent for specific procedures or onward referral where applicable; and
- correspondence with other healthcare workers that relates to the patient's care.

As an employer, the practice also processes the personal data of employees, including:

- personal information and contact details, including name, address and date of birth;
- health clearance and immunisation status where relevant;
- employment and educational histories;
- absence/leave records;

- performance and appraisal information; and
- information on training and professional development.

This data is kept for two years after employee termination.

Procedures for Ensuring Compliance with the UK GDPR and the Confidentiality and Security of Personal Data

All Staff including associate Doctors

To maintain a good patient–medical team relationship, it is essential that patients feel they can provide personal information to medical team members with the knowledge that this information will be kept securely and not shared unlawfully. It is also important that patients are able to provide, in confidence, full details of their medical and social histories to facilitate safe and effective care.

To achieve this, all staff must follow the procedures listed below.

- Comply with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, relevant confidentiality requirements, applicable Caldicott Principles and General Medical Council professional standards.
- Undergo appropriate training in processing personal data, confidentiality and information security.
- Keep any personal data or confidential data that they hold, whether in electronic or paper format, securely, which includes:
 - storing paper files with personal data in lockable filing cabinets that are locked when authorised staff are not present to monitor access;
 - storing electronic files containing personal data on authorised, password-protected computer systems;
 - screen-locking unattended computers. All workstations will automatically lock after 2 minutes if not used;
 - not sharing computer passwords with unauthorised people or writing down passwords in insecure locations;
 - using strong, unique passwords and multi-factor authentication where provided;
 - not forwarding personal or confidential information to personal email accounts or unauthorised systems;
 - holding personal data on laptops or portable devices only where there is a clear business necessity and appropriate authorisation. Devices containing personal data must be appropriately encrypted;
 - avoiding carrying personal data on removable media such as memory sticks unless specifically authorised and appropriately secured;

- not using unlicensed or unauthorised software on practice computers;
- not using personal messaging or social media applications to communicate identifiable patient information unless expressly authorised by the practice and appropriate data protection and security safeguards are in place;
- ensuring windows and doors are secured if you are the last to leave the practice; and
- reporting lost devices, suspected compromise of passwords or other information security incidents immediately.
- Practice good record-keeping, and ensure records are:
 - accurate;
 - dated;
 - contemporaneous;
 - comprehensive;
 - secure;
 - attributable to the person making the entry;
 - legible and written in language that can be read and understood by others and is not derogatory; and
 - amended in a manner that preserves an appropriate audit trail.
- Maintain the confidentiality of any personal data by, for example:
 - ensuring that personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party;
 - avoiding working on identifiable personal data in public places where information could be viewed or overheard;
 - not discussing identifiable information about patients with anyone outside the practice unless there is an appropriate lawful and confidential basis for doing so;
 - not leaving inappropriate messages about a patient's care with an unauthorised third party;
 - respecting patient privacy for discussions of a sensitive nature, including medical information and payment information; and
 - recognising that confidentiality obligations continue after termination of employment or engagement.

- Ensure patients are provided with appropriate information about how their personal information is used and shared through the Practice's Privacy Notice and other appropriate communications.
- Share personal data only where there is a lawful and appropriate basis for doing so, where the sharing is necessary and proportionate, and on a need-to-know basis. Only the minimum information necessary will be shared. Depending upon the circumstances, information may be shared:
 - with another health professional for the provision of effective care and/or treatment;
 - with a laboratory for the processing of test samples; or
 - with another appropriate organisation where there is a lawful basis and the sharing is necessary for the provision or management of healthcare.

Patient consent will be obtained where required or appropriate, but staff must not assume that consent is the lawful basis for every disclosure of patient information.

- Check that any personal information that you provide in connection with your employment is accurate and up to date and inform the Practice Manager of any changes to this information.
- Inform the Practice Manager/Data Protection Lead immediately of any suspected or actual personal data breach, confidentiality breach or information security incident.

Data Controllers

Data controllers are organisations or individuals who determine the purposes and means of processing personal data. The practice will clearly document controller arrangements and will not rely on the concept of a doctor "owning" a patient list as the basis for determining controller status.

All data controllers must follow the procedures detailed above for staff and the procedures listed below.

- Where the practice is required to pay the ICO data protection fee, the practice will ensure that the fee is paid and that relevant details are kept up to date.
- Maintain appropriate records of processing activities where required.
- Ensure that appropriate Privacy Notices are maintained.
- Ensure that data protection risks are assessed and that Data Protection Impact Assessments (DPIAs) are undertaken where required.
- Ensure that appropriate technical and organisational measures are in place to protect personal data.
- Ensure that processors are appropriately assessed and governed and that appropriate written contracts are in place where required.

- Ensure that personal data breaches are assessed, recorded and notified to the ICO and/or affected individuals where legally required.
- Ensure that personal data is retained and securely disposed of in accordance with the Practice's Records Management and Retention arrangements.

General Medical Practice

All staff contracts and agreements include a clause regarding confidentiality of personal data.

- Keys for lockable storage cabinets are held only by medical team members who require regular access to the information they contain. Keys are stored in a safe place/secure key cabinet which is secured to the wall in the reception cupboard.
- Practice workstations have appropriate audit trail facilities to identify access, amendments and other relevant activity within the patient management system.
- All workstations are password protected and access to patient software systems is by MFA.
- The practice uses appropriate password and authentication controls and will review these periodically in accordance with information security requirements.
- Each computer is fitted with appropriate anti-virus software.
- Back-ups of the practice's patient software records are made regularly throughout the day as our system is cloud based, (back-up is made to Amazon based servers located in the UK) and this allows for quick retrieval of information.
- Back-ups are tested by our IT provider to ensure data can be retrieved in a usable format.
- GP record for an individual must be held for the lifetime of the patient, and ten years after death.
- Personal data are reviewed, updated, retained and securely deleted or destroyed in a confidential and secure manner when no longer required.
- Windows are fitted with locks and the practice is fitted with an intruder alarm that is set each night to increase security.
- Access to practice information systems is provided on a role-based and least-privilege basis. Access will be removed or amended promptly when staff leave the practice, change roles or no longer require access.
- A continuity plan that includes procedures for protecting and restoring personal data is in place in the event of a major incident.
- The practice will undertake appropriate due diligence and oversight of third-party suppliers who process personal data on behalf of the practice.

- Where a third-party acts as a data processor, the practice will ensure that an appropriate written contract containing the required data protection provisions is in place.
- The practice will consider whether a Data Protection Impact Assessment is required before introducing new processing activities which are likely to result in a high risk to individuals.
- The practice will maintain appropriate records to demonstrate compliance with its data protection obligations, including, where applicable, records of processing activities, data breaches, training, DPIAs and data protection risk assessments.

Sharing Personal Information

To provide patients with appropriate care, we might need to share personal data with:

- another health professional who is caring for the patient;
- the patient's NHS GP;
- a medical laboratory;
- a private health/medical scheme if the patient is a member;
- other healthcare providers involved in the patient's care; and
- appropriate service providers acting on behalf of the practice where necessary and lawful.

To fulfil our duties as employers, we might need to share staff personal data with:

- other employers where lawful and appropriate;
- HM Revenue & Customs;
- pension providers;
- educational institutions;
- regulatory and professional bodies; and
- other organisations where there is a lawful and necessary reason for sharing.

In these cases, only the minimum information required will be shared and the practice will consider the lawful basis, confidentiality requirements and any applicable consent or authorisation before disclosure.

Where organisations process personal data on behalf of the practice, the practice will undertake appropriate due diligence and ensure that suitable contractual and security arrangements are in place.

Disclosure Without Consent

Exceptional circumstances might override the duty to maintain confidentiality. Where possible and appropriate, we will inform the patient or staff member of requests to share personal information.

The decision to disclose information without consent must be taken by an appropriately authorised senior member of staff/clinician, taking into account the circumstances, the duty of confidentiality, applicable professional guidance and the relevant legal requirements.

Examples include:

- situations where there is a serious public health risk or risk of harm to other individuals;
- where information is lawfully required for the prevention or detection of crime or the apprehension or prosecution of offenders;
- in response to a valid court order or other legal requirement;
- where disclosure is otherwise permitted or required by law;
- to enable the practice or a clinician to pursue or defend a legal claim where disclosure is lawful and necessary; and
- other circumstances where the law permits or requires disclosure without consent.

Requests from the police, courts, solicitors, insurers, regulators or other third parties will be assessed on a case-by-case basis. The practice will establish the identity and authority of the requester, determine whether there is a lawful basis for disclosure, consider the duty of confidentiality and disclose only information that is necessary and proportionate.

Dr David Richardson is responsible for making or overseeing decisions regarding whether personal data should be disclosed, subject to appropriate clinical, legal or professional advice where necessary.

Data Breaches

We will always aim to ensure that the information we hold is kept securely.

All suspected or actual personal data breaches and information security incidents must be reported immediately to the Practice Manager/Data Protection Lead so that they can be assessed and managed appropriately.

The practice will assess each personal data breach to determine the likelihood and severity of any risk to the rights and freedoms of individuals.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the practice will notify the ICO without undue delay and, where required, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, the practice will notify those individuals without undue delay where required by law.

Not every confidentiality or information security incident will require notification to the ICO. The Practice will undertake and document an appropriate risk assessment to determine whether notification is required.

We will document all personal data breaches, including those that are not notifiable to the ICO, and will include information regarding the nature of the breach, its effects, the risk assessment, the steps taken to mitigate any adverse effects and the measures implemented to prevent recurrence.

Data Subject Rights

We recognise the rights of individuals under the UK GDPR and have processes in place to deal with relevant requests.

We provide Privacy Notices to comply with an individual's right to be informed.

Where an individual requests access to their information, we will normally provide access without undue delay and within the applicable statutory timeframe. A Subject Access Request will normally be responded to within one month of receipt, subject to the applicable legal requirements. Where permitted by law, the practice may extend the response period where a request is complex or where other statutory provisions apply.

The practice will not charge a fee for a standard Subject Access Request. A reasonable fee may be charged, or a request may be refused, where the law permits this because a request is manifestly unfounded or excessive. Any decision to refuse or restrict a request will be documented and explained to the individual together with information about their rights to complain to the ICO and seek legal advice.

Where an individual notifies us that the information we hold about them is inaccurate, we will consider and rectify inaccurate personal data without undue delay where appropriate.

Where an individual asks us to delete their information, we will consider the request in accordance with the right to erasure and any applicable legal, regulatory, professional or contractual obligations to retain the information. The right to erasure is not absolute.

Where an individual asks us to restrict processing, we will consider the request in accordance with the applicable UK GDPR requirements.

Where an individual asks us to transfer their information to another medical practice, we will consider whether the right to data portability applies. Where applicable, information will be provided or transferred in a structured, commonly used and machine-readable format or otherwise handled in accordance with the applicable legal requirements.

Individuals also have the right to object to certain processing. The practice will consider objections in accordance with the applicable UK GDPR requirements and the lawful basis being relied upon.

The practice does not currently use solely automated decision-making, including profiling, to make decisions concerning patients or staff that produce legal or similarly significant effects. If this changes, the practice will assess the processing against the applicable UK GDPR requirements and safeguards.

Individuals may also make a data protection complaint to the practice. The practice maintains a separate Data Protection Complaints Policy setting out the procedure for making, acknowledging, investigating and responding to such complaints. The practice will provide a clear route for individuals to raise data protection complaints and will deal with complaints in accordance with applicable legal requirements.

Where an individual remains dissatisfied following the practice's handling of a data protection matter, they may have the right to complain to the Information Commissioner's Office (ICO).