# DATA PROTECTION POLICY

| VERSION CONTROL | |
|---|---|
| **Version** | 1 |
| **SLT Sponsor** | Information Governance Group |
| **Owner** | Governance, Risk and Compliance |
| **Approving Committee and Date** | Information Governance Group ("IGG")<br>September 2025 |
| **Effective Date** | October 2025 |
| **Periodic Review Date** | Please note: As of 19 June 2025, the Data (Use and Access) Act (DUAA) became law in the UK. The DUAA is a new Act of Parliament that updates some laws about digital information matters, it amends but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR). It will be phased in from June 2025 and June 2026 and this Policy will remain under review during that time. |

## 1. Introduction

Data Protection is the fair and proper use of information about living individuals, who are known or referred to as 'Data Subjects. In the United Kingdom, the Data Protection Act ("DPA") 2018, the UK General Data Protection Regulation ("UK GDPR") and the Privacy and Electronic Communications Regulations ("PECR") regulates the way in which information about individuals is handled. Collectively, this is referred to or known in this Policy as 'data protection legislation.'

As part of its activities, The Royal College of Surgeons of Edinburgh ("RCSEd") collects, uses, shares, retains and destroys personal data about its members, staff and others in order to deliver services, exercise its duty of care and fulfil its contractual and legal obligations.

## 2. Purpose

**2.1** This policy and its supporting procedures and guidance support RCSEd comply with its obligations as a Data Controller and where applicable, a Data Processor, under the data protection legislation.

Primarily, under the data protection legislation, RCSEd is responsible for and must be able to demonstrate compliance with the following Data Protection Principles:

- Accountability
- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

This policy details how the RCSEd follows data protection best practice in carrying out its activities. It sets out what RCSEd's employees and volunteers must do when any personal data belonging to, or provided by, members, staff or others is collected and processed.

## 3. Objectives

The key objective of this policy is to ensure that the Data Protection Principles, as seen above, and other requirements considered under the data protection legislation are met by RCSEd. RCSEd will apply the following objectives through the information life cycle to commit to protecting data held, shared and received by the RCSEd.

### 3.1 Process personal data lawfully and fairly

To collect and process personal data for any specific purpose, RCSEd must always have a lawful basis to do so. RCSEd will only collect and process personal data personal data in accordance with lawful terms stated under the UK GDPR, Article 6.

This means, at least one of the following must apply:

- **Consent** must have been given by the data subject for one or more specific purposes.
- The processing is necessary for the **performance of a contract** to which the subject is party to.
- RCSEd must comply with **legal obligations.**
- The **vital interest** of the data subject or another person must be protected, for example where processing is necessary to protect the individual's life.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (**public task**), for example special category personal data or criminal offences personal data.
- Processing is necessary for the purpose of **legitimate interests** by RCSEd, where such interests are overridden by the interests or fundamental rights of the data subject.

**Consent** as a condition for processing personal data can only be relied on when the consent has been given **specifically, informed and freely given** by the data subject. Consent needs to be documented in a clear statement or affirmative action (written statement, electronic means or an oral statement). Consent can be **withdrawn** at any time without harm to the data subject's interests.

**Legitimate interests** is a lawful basis for data processing under UK GDPR; however, it differs from other lawful bases as it is not centered around a particular purpose, and it is not processing that the individual has specially agreed to (consent). This means the processing of personal data can be done in RCSEd's own interests, **as long as the interests or fundamental rights and freedoms of the data subject are not compromised**. It may be appropriate to use legitimate interest when the processing is not required by law but has a clear benefit to the parties involved, there is limited privacy impact on the individual and the individual reasonably expected their data to be used in that way. RCSEd may use 'legitimate interest' when it comes to direct marketing.

### 3.2 Transparency with data subjects

RCSEd is required to inform data subjects how their personal data will be processed in **a clear, concise and accessible way**. The RCSEd's Privacy Policy or appropriate Privacy Notice, outlines how personal data is being used by RCSEd. RCSEd will proactively inform data subjects about its data processing activities and their rights under the law.

The Privacy Policy is published on the RCSEd website and the content of the policy reviewed regularly. Data subjects will be informed of any significant changes that may affect them.

Data subjects will be kept informed about any RCSEd news, activities and events; and each communication that a data subject receives will have an option to opt out of any further marketing communications.

In doing so, RCSEd will provide accountability for the use of personal data and demonstrate compliance with UK GDPR principles and PECR.

### 3.3 Upholding the rights of data subjects

Data subjects have the right to hold RCSEd accountable for any personal data collected and processed.

**Right to be Informed**

- RCSEd will provide data subjects with information about what data is being collected, for how long and what RCSEd intend to do with that data.

**Right of Access**

- Data subjects will have the right to obtain copies of their personal data free of charge within one month of their request, this is commonly known as a Subject Access Request (SAR). The deadline can be extended by two months in the case of complex or voluminous requests.

**Right to Rectification**

- RCSEd will rectify any inaccurate or incomplete personal data held on a data subject within one month of the request.

**Right to Erasure**

- RCSEd will erase any personal data held on a data subject that is no longer necessary, the data subject has withdrawn consent, or the data was processed unlawfully. This is also known as the **right to be forgotten.**

**Right to Restrict Processing**

- RCSEd will restrict the processing of personal data until a dispute about the data's accuracy or use has been resolved. Personal data no longer needed to be kept but the data subject needs the data for a legal claim, or a data erasure request has been submitted to RCSEd.

**Right to Data Portability**

- RCSEd will provide the data subject with their personal data in a structured, usable, machine-readable format. Examples include CSV, XML and JSON files.

**Right to Object to Processing**

- Data subjects have the right to object and prevent further data processing of their data under the RCSEd's legitimate interests or public interest, unless RCSEd can demonstrate lawful grounds to continue. For example, a data subject can object to data being shared for marketing purposes.

**Right to Automated Decision Making and Profiling**

- Data subjects have the right to object to data processing if it is solely automated (no human interaction).

### 3.4 Protecting personal data

RCSEd will handle personal data in a manner that ensures data protection by design and default, ensuring appropriate technical and organisational measures are in place throughout the entire lifecycle of personal data. Under **Article 25**, it states only personal data necessary for each specific purpose of processing is processed. This means RCSEd will reduce risks of disclosure by anonymising and pseudonymising personal data where possible, limiting information held, and restricting access, sharing and retention of personal data. Data Protection Impact Assessments (DPIA) will be used to identify and mitigate privacy risks, where appropriate.

RCSEd will apply a "privacy first" approach to any settings of systems and applications. RCSEd will only use data processors (third parties) that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will comply with data protection law and protection the rights of the data subject.

RCSEd will require all staff and a proportion of volunteers to undertake basic data protection training, supplemented by procedures and guidance relevant to a specific role. Furthermore, it will ensure staff and volunteers are aware of how data protection law applies to their role and responsibilities.

In line with the development of a Retention Policy, RCSEd will keep records and information containing personal data only so long as required for the purposes for which they were collected.

### 3.5 Managing breaches promptly and appropriately

RCSEd will take all necessary steps to reduce the impact of breaches involving personal data. RCSEd has put in place appropriate procedures to deal with any personal data breaches and, where required by law, will notify the Information Commissioner's Office (ICO) and/or other data subjects of breaches.

If a breach or suspected breach occurs, the Governance, Risk and Compliance (GRC) team must be alerted immediately. The GRC team will take all appropriate steps to preserve evidence relating to the breach and provide advice and relevant next steps and actions to the individual or team that reported it.

Please see the Personal Data Breach Policy/Guidelines.

## 4. Scope

### 4.1 What is included in the policy

This policy applies to all personal data that the RCSEd processes regardless of the format or media on which the data are stored or who it relates to.

The policy applies to all locations from which RCSEd personal data is accessed and processed, including home use.

RCSEd is a global network operating internationally through arrangements with partners in other jurisdictions. As such, the remit of the policy includes international activities and will take into consideration non-UK legislation that might be applicable. At present, the College is exploring when

the Malaysian Personal Data Protection Act 2010 may apply.

### 4.2 Who is covered in the policy?

**Data Subjects**

These include, but are not confined to: prospective, current and former members, fellows, affiliates, current and former employees, current and former volunteers, current and former Charity Trustees, family members where emergency or next of kin contacts are held, workers employed through temping agencies, potential and actual donors and funders, customers, conference delegates, course delegates, people making requests for information, complainants, contractors, suppliers and partners.

**Users of personal data**

The policy applies to anyone who obtains, records, accesses, stores or uses personal data in the course of their work for the RCSEd. Users of personal data include but are not limited to: Charity Trustees, employees, volunteers, contractors, suppliers and partners.

## 5. Who is responsible for the Policy

The policy is owned by the Governance, Risk and Compliance team. It is sponsored and approved by the College's Chief Executive Officer on behalf of the Senior Leadership Team, with ultimate authority for delivery resting with the Information Governance Group.

## 6. APPENDICES

### 6.1 Roles and Responsibilities

**All users[1] of RCSEd information are responsible for the following:**

- Completing relevant training provided by RCSEd to support with the compliance of the policy.
- Considering and taking all necessary steps to ensure no data breaches occur as a result of their actions.
- All suspected breaches or incidents are reported to dataprotection@rcsed.ac.uk so appropriate actions are taken, and any risk or harm is minimised.
- Informing RCSEd of any changes to information held by RCSEd, for example address or bank account details.

**The RCSEd Board of Trustees**

The RCSEd Board of Trustees has ultimate accountability for RCSEd's compliance with data protection law and the Act.

[1] All the RCSEd Charity Trustees, employees or volunteers

**The Chief Executive Officer ("CEO")**

The CEO has senior leadership accountability for the RCSEd Board of Trustees, chairing the Information Governance Group ("IGG") and for ensuring the Head of Governance, Risk and Compliance has sufficient resources to carry out their responsibilities effectively.

**Information Governance Group ("IGG")**

The IGG is the operational body responsible for developing and overseeing a comprehensive and effective Information Governance Framework which will ensure that best practice is in use within RCSEd, in line with current legislation and promotes best practice being developed within RCSEd. It is responsible for reviewing the effectiveness of data protection and information governance policies and procedures.

**Head of Governance, Risk and Compliance**

The Head of Governance, Risk and Compliance, has responsibility for data protection and information governance within RCSEd and reports to the CEO.

With the involvement of IGG, they are responsible for:

- informing and advising the senior leadership team (SLT) and staff about their obligations to comply with current legislation.
- promoting a culture of data protection, through organising training and providing informative material.
- providing advice and expertise on data protection-related matters.
- monitoring compliance with relevant data protection laws.
- being the first point of contact for supervisory authorities and for individuals whose data is processed.
- investigating personal data breaches, recommending actions to reduce the impact and likelihood of recurrence.
- advising on data impact assessment and monitoring its performance.

**The Governance, Risk and Compliance team** or **members of IGG** will take on the responsibility listed above, as directed.

The College maintains a separate information security framework, overseen by the **Head of Digital Information & Infrastructure** & the **Head of Applications and Online Services**, who are core members of the IGG.

**Directors and Heads of Department and Managers**

All Directors and Senior Managers are responsible for implementing the policy within their business area and for adherence by their staff.

**Information Asset Owners ("IAOs")**

IAOs are senior/responsible individuals involved in the management of the business. They are responsible for constructing and maintaining information in their area, for managing and controlling access to the data, for ensuring that data is complete and accurate, and for raising awareness about data protection within their teams.

## 7. Definitions

| | |
|---|---|
| **Personal data** | Personal data is data which relates to a living individual who can be identified:<br>from that data; or<br>from that data and other information, which is in the possession of, or is likely to come into the possession of, the Data Controller; and which is in electronic form or held manually (paper record) in a relevant filing system.<br><br>This definition also includes any expression of opinion about the individual Data Subject and any indication of the intentions of the Data Controller or any other person in respect of the Data Subject. |
| **Sensitive Personal Data** | Sensitive personal data is personal data about an identifiable individual's:<br>• racial or ethnic origin;<br>• political opinions;<br>• religious beliefs, or other beliefs of a similar nature;<br>• trade union membership;<br>• physical or mental health;<br>• sexual life; and/or<br>• proven or alleged offences, including any legal proceedings and their outcome.<br>• Genetic or biometric data when processed to identify that individual |
| **Data Controller** | A Data Controller determines the purposes and means of processing personal data. This means the data controller makes decisions about how personal data is collected, used and managed. They are responsible for ensuring processing activities comply with the UK GDPR. |
| **Data Processor** | Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. |
| **Processing** | Includes, but is not limited to: creating, storing, accessing, using, sharing, disclosing, altering, updating, destroying or deleting personal data. |
| **Third Party** | Any individual or organisation other than the Data Subject or the Data Controller**.** |

| | |
|---|---|
| **Pseudonymisation** | Refers to techniques that replace, remove and transform information that identifies people, and keep that information separate. |

**Related College Policies or Procedures:**

- Privacy Policy and Associated Privacy Notices (see the website)
- Information Security Policy
- CCTV Policy
- Procedure to be Followed in the Reporting Data Protection Breaches
- Procedure to be Followed in Response to Subject Access Requests
- Procedure to be Followed in Response to Request to Erase Personal Data
- Procedure to be Followed in Response to Requests to Rectify Personal Data
- Procedure to be Followed in Response to Requests to Restrict the Processing of Personal Data
- Guidance on Development Data Sharing Agreements