FROM HERE, HEALTH

THE ROYAL COLLEGE OF SURGEONS OF EDINBURGH

Data Protection Policy

May 2018

Approving authority	Senior Management Team
Approval date	24 May 2018
Effective date	24 May 2018
Review period	One year from date of approval
Policy owner	Information Governance Group

1. INTRODUCTION

The Data Protection Act 1998 ("the Act") regulates the way in which information about living individuals ("Data Subjects") is collected, stored or transferred. Compliance with the Act is important because a failure to adhere to its terms presents significant legal, reputational or financial risks for The Royal College of Surgeons of Edinburgh ("RCSEd"), or indeed in exceptional circumstances, for individual Charity Trustees (RCSED Council Members), employees and volunteers.

As part of its activities, RCSEd collects, uses, shares, retains and destroys Personal Data about its members, staff and others in order to deliver services, exercises its duty of care and fulfil its contractual and legal obligations. All personal information must be collected, stored, used and disposed of properly, in accordance with the principles of the Act.

For ease of reference, the defined terms are explained in the appendix at section 4 of this policy.

1.1. Purpose

The purpose of this policy is to set out the principles of data protection best practice which RCSEd will follow, and to provide a managed framework for fulfilling business needs, accountability and legal responsibility. It sets out what RCSEd's Trustees, employees and volunteers must do when any Personal Data belonging to, or provided by, members, staff or others is collected, stored or transmitted onwards.

1.2. Scope

1.2.1. What information is included in the policy?

The policy applies to all Personal Data created, received, held and shared in the course of RCSEd business in all formats (paper or electronic) at any time.

1.2.2. Who is affected by the policy?

Data Subjects

These include, but are not confined to: prospective, current and former members, fellows, affiliates, trainees, younger fellows, RSAs, RDAs, ISAs, IDAs, 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, courses 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.

1.2.3. Where does it apply?

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.

1.3. Lines of Responsibility

1.3.1. The RCSEd Council ("Charity Trustees")

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

1.3.2. Deputy Chief Executive of RCSEd

The Deputy Chief Executive is the designated Data Protection Officer who is responsible for informing the RCSEd and its employees about their obligations to comply with the Act; monitoring compliance with the Act and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits; and being the first point of contact for supervisory authorities and for individuals whose data is processed. He reports to the RCSEd Council and the Audit Committee on relevant risks and issues.

1.3.3. Information Governance Group ("the Group")

The Group develops and oversees a comprehensive and effective Information Governance Framework which will ensure that best practice is in use within RCSEd, and that it is compliant with current legislation.

1.3.4. Directors and Senior Managers

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

1.3.5. IT Team/AOS Team

The IT & AOS teams are responsible for ensuring the implementation of the policy with regard to access to and functionality of Business Information Systems within RCSEd as well as the secure backup and storage of data covered by the policy.

1.3.6. All users of RCSEd Information

All the RCSEd Charity Trustees, employees or volunteers are responsible for:

- handling Personal Data in accordance with the principles of the Act;
- undertaking relevant training provided by RCSEd to support compliance with this policy;
- taking necessary steps to ensure that no breach of information security result from their actions;
- reporting all information security breach, or non-compliance with this policy, to the Data Protection Officer for RCSEd.

1.4. Related Policies and Procedures

The following policies are currently being formulated within RCSEd:

- Records Management Policy
- Information Security Policy
- CCTV Policy
- Data Protection Procedures
- Reporting Data Protection Breaches
- Privacy Policy

1.5. Reference Documentation

- Data Protection Act 1998 ("the Act"): https://ico.org.uk/for-organisations/guide-to-data-protection/
- CCTV Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- General Data Protection Regulation (2018): https://ico.org.uk/for-organisations/data-protection-reform/
- Malaysia: Personal Data Protection Act (2010): http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf

2. POLICY

2.1. Notification to the Information Commissioner Office ("ICO")

As a Data Controller, RCSEd will update the details on the ICO's register on an annual basis. RCSEd's notification on the Register of Data Controllers is published on the ICO's website: https://ico.org.uk/ESDWebPages/Entry/Z5731683
This includes details of the data processed by RCSEd.

2.2. Policy objectives

When processing Personal Data, RCSEd will comply with the Act and its eight principles. The principles say that Personal Data must:

- Be processed fairly and lawfully;
- Be obtained for specific and lawful purposes;
- Be adequate, relevant and not excessive in relation to the purpose for which it is used;
- Be kept accurate and up to date;
- Not be kept for longer than is necessary for the purpose for which it is used;
- Be processed in accordance with the rights of Data Subjects;
- Be kept secure to prevent unauthorised processing and accidental loss, damage or destruction; and
- Not be transferred to any country outside the EEA (unless an exception applies).

2.2.1. Fair and lawful

RCSEd will not use Personal Data in ways that have unjustified adverse effects on the Data Subjects concerned; handle Data Subject's Personal Data only in ways they would reasonably expect; and make sure not to do anything unlawful with the Personal Data.

RCSEd will adhere to a principle of transparency and tell Data Subjects what it will do with the information it holds about them at the point of collection. The Data Subject will be given appropriate privacy notices and will be told:

- who the Data Controller is, i.e. RCSEd;
- the purpose or purposes for which their Personal Data is being processed;
- any other information to make the processing fair.

Data Subjects' explicit consent will be obtained and recorded as necessary in relation to each of RCSEd's uses, and any secondary uses, of their Personal Data.

Personal Data will only be disclosed to those organisations and individuals who the Data Subject has consented may receive his or her Personal Data, or to organisations that have a legal right to receive the Personal Data without consent being given.

2.2.2. Specific and lawful purposes

RCSEd will collect and use Personal Data only in accordance with the purposes stated in its notification to the ICO, and with those described to the Data Subjects at the time of collecting the information.

The Data Protection Officer should be advised in writing of any plans to process data of classes or purposes not covered in RCSEd's registered entry on the ICO's website, or of any amendments required to it as early as possible. A failure to do so, or knowingly to process data other than in accordance with the registered entry, may constitute an offence under the Act.

2.2.3. Adequate, relevant and not excessive

RCSEd will ensure to collect Personal Data that is sufficient for the purpose it is collected it for; and will not hold more information than needed for that purpose.

2.2.4. Accurate and up to date

RCSEd will take reasonable steps to ensure the accuracy of any Personal Data obtained; ensure that the source of any Personal Data is clear; carefully consider any challenges to the accuracy of information; and consider whether it is necessary to update the information and/or the consent of the Data Subjects.

It is the responsibility of each individual employee to notify their line manager of any changes. In the absence of evidence to the contrary, it will be assumed that the information is up to date.

2.2.5. Retention

RCSEd will put in place a retention schedule setting out how long particular types of data need to be kept for. It will securely delete or supress information that is no longer needed and will update, archive and securely delete or supress information if it goes out of date.

2.2.6. Data Subjects' Rights

A Data Subject has certain rights conferred under the Act, including:

- to request access to his or her Personal Data; and
- to prevent processing likely to cause damage or distress.

A Data Subject may request access to all Personal Data of which he or she is the subject upon payment of a £10 fee ("Subject Access Request").

This Subject Access Request must be made in writing and the statutory deadline for providing a response is 40 calendar days. There are exemptions from the access rules in certain limited circumstances.

RCSEd will respond properly and promptly to Subject Access Requests, and will carefully consider requests for data to be amended or for processing to be suspended.

2.2.7. Data Security

RCSEd will take appropriate technical, physical and organisational measures to ensure that the information is held securely and safeguarded from destruction, loss, unauthorised access and disclosure.

The RCSEd will issue an Information Security Policy containing guidance in relation to data security and how Personal Data should be processed and transferred securely.

2.2.8. International Transfers

The RCSEd will not transfer data outside of the EEA except for legitimate purposes, e.g.:

- the data protection arrangements in the destination country have been approved by the EU Commission; or
- the recipient is a signatory to an EU approved data protection regime; or
- the recipient is bound by a contract that ensures that the data concerned will be adequately protected.

Given the links that RCSEd maintains with other countries around the world, some Personal Data may fall into this category. Therefore, prior to transferring data outside the EEA or giving anyone outside the EEA access to Personal Data, the Data Protection Officer must be contacted.

2.3. Reporting breaches

RCSEd recognises that mistakes can happen and will implement an internal policy to ensure that members of staff know what to do in the event of a breach of the Act.

Breaches will be reported by the Data Protection Officer to the ICO where required by the Act.

2.4. Sensitive Personal Data

Sensitive Personal Data can only be processed under strict conditions including the explicit consent of the Data Subject concerned, unless a specific exemption applies. Therefore, if Sensitive Personal Data is collected and processed, appropriate steps will need to be taken to ensure that the necessary explicit consent of the Data Subject has been given to process his or her Sensitive Personal Data.

3. IMPLEMENTATION

3.1. Implementation

This policy will be implemented through the development, communication, monitoring and review of the RCSEd's information security plan including:

- an information audit;
- related policies (records management and retention schedules; privacy policy; CCTV policy);
- related procedures and toolkits; and
- a training plan for staff.

3.2. Monitoring and Evaluation

The policy will be monitored by RCSEd's Information Governance Group. An Information Security Risk Register will be developed and monitored. Incidents will be reported to and logged by the Data Protection Officer.

3.3. Review

The Information Governance Group will review this policy, and related policies, every year to ascertain its continuing relevance and effectiveness in the light of any legislative or other developments. Any substantive changes will be notified by appropriate means to all concerned.

4. APPENDIX: DEFINITIONS

Personal Data
Personal Data is data which relates to a living individual who can be identified:

- from that data; or
- 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.

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:

- racial or ethnic origin;
- political opinions;
- religious beliefs, or other beliefs of a similar nature;
- trade union membership;
- physical or mental health;
- sexual life; and/or
- proven or alleged offences, including any legal proceedings and their outcome.

Data Subject
An individual whose Personal Data is held by RCSEd – or any other organisation.

Data Controller
A person or organisation who determines the purposes for which Personal Data is processed, and is legally accountable for the Personal Data it collects and uses or contracts with others to process on its behalf; in this case, RCSEd.

Data Processor
Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

Processing
Creating, storing, accessing, using, sharing, disclosing, altering, updating, destroying or deleting data.

Third party
Any individual or organisation other than the Data Subject or the Data Controller.