Data Protection Complaints Procedure

DOCUMENT INFORMATION	
Title:	Data Protection Complaints Procedure
Purpose:	To provide individuals with a clear, structured method to raise concerns about how their personal information is handled by the Group. It is designed to ensure the existence of clear processes to investigate mishandling, resolve issues transparently, and adhere to statutory legal requirements.
Target Audience:	All users and visitors to the College, Museum and Surgeons Quarter (SQ) (including trustees, employees, volunteers, visitors contractors and sub-contractors)
Superseded Documents:	N/A
Related Documents: *(non-exhaustive list)*	Data Protection Policy

VERSION CONTROL	
Version	1.0
SLT Sponsor	Mark Egan
Owner	Governance, Risk and Compliance
Approving Committee	Information Governance Group
Effective Date	17/06/26
Periodic Review Date	Date of approval + 2 years

DOCUMENT HISTORY					
Document History Version	**Owner**	**Author**	**Status**	**Change**	**Date**
1.0	IGG	Records Manager	Approved		June 2026

The Royal College of Surgeons of Edinburgh and Surgeons Quarter (The Group) Data Protection Complaints Procedure

From 19 June 2026 every UK organisation acting as a data controller must operate a data protection complaints process. The Information Commissioners Office (ICO) frames this as five core duties:

1. **Provide a clear, accessible route to complain:** an email address, online form, portal or postal route is acceptable, but it must work for the intended audience, with extra care for children and vulnerable people.
2. **Inform people of their right to complain** both to the organisation and to the ICO. This must appear in privacy notices (when data is collected) and in responses to Subject Access Requests (SARs).
3. **Acknowledge within 30 days of receipt:** a simple acknowledgement (an auto reply is fine for electronic complaints), not a full response.
4. **Investigate without undue delay:** meaning no "unjustifiable or excessive" delay, judged on complexity, scale and any harm being suffered. Internally set service standards must not be used to slow things down, and enquiries and decisions must be recorded and justified.
5. **Communicate the outcome without undue delay:** explain any remedial action and remind the complainant of their right to escalate to the ICO.

2. Purpose

This procedure sets out how the Group handles complaints about its processing of personal data, in compliance with the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and the Privacy and Electronic Communications Regulations 2003. It should be read with RCSEd's Data Protection Policy and Privacy Notices.

Definitions

- **Personal data:** information relating to an identifiable living individual.
- **Data subject:** the individual the personal data relates to (staff, Members, Fellows, volunteers, visitors, and individuals captured by CCTV).
- **Data controller / processor:** the body determining the purposes of processing / a body processing on its behalf.
- **Data protection complaint:** any expression of dissatisfaction about how the Group has handled personal data.

Scope

A complaint may relate to the handling of the complainant's personal data by RCSEd, SQ, or a processor acting for it; a data breach affecting the complainant; RCSEd's or SQ's response to a rights request such as a SAR; the handling of an earlier request or complaint; or the content of a current privacy notice. Complaints may be made by the data subject or by a representative acting with the data subject's written authority.

How to make a complaint

Complaints should be sent to the Governance Risk and Compliance Team at dataprotection@rsced.ac.uk

To help us investigate, please describe:

- the issue in your own words
- what happened and when
- whether you have already raised it with anyone at RCSEd or SQ and whom
- how the matter has affected you
- what outcome would resolve it for you
- include relevant correspondence

Timeframes and time limits

- **Acknowledgement:** we will acknowledge your complaint within 5 working days (and in all cases within the 30 days required by law). During institutional closures this acknowledgement this may take slightly longer, but never beyond the legal limit.
- **Investigation and outcome:** we will investigate without undue delay and aim to provide an outcome within one calendar month. If the matter is complex, we may need more time however, we will tell you and keep you updated on progress and expected timescales.
- **Time limit:** we have discretion not to investigate matters raised more than three months after the events complained of (or your last meaningful contact about them), as the passage of time can make a fair investigation impractical. We will consider complaints outside this window where there is good reason.

3. Identity and authority

Where there is any doubt about identity, we may ask for proof (e.g. a copy of a passport or photo driving licence) before proceeding. Where a representative complains on someone's behalf, we will require written authority from the data subject. A child may exercise these rights on their own behalf as long as they are competent to do so. In the case of children under 12 behalf of a child, you must provide proof of your own identity, proof of your relationship to the child. In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights. Complaints from third parties are considered on a case-by-case basis.

4. Stages

Stage 1: Informal resolution. Wherever possible we will try to resolve the complaint quickly and informally with the team that handled the original matter. Most complaints can be resolved this way.

Stage 2: Formal review. If you are dissatisfied with the informal outcome, you may ask the CEO in writing to review it, providing supporting information. An appropriate reviewing officer will investigate and the CEO (or a senior nominee) will respond in writing as the final arbiter.

5. Investigation

We will look at the relevant facts thoroughly, fairly and proportionately which may include speaking to staff, reviewing records, and checking whether we have met our own policies and standards. We will keep our enquiries proportionate, and record our process, enquiries and decisions so they can be justified. We will keep you informed throughout this process.

6. Outcomes

Depending on our findings, outcomes may include: an explanation of how and why data was processed; an acknowledgement and apology where an error or breach occurred; remedial action (e.g. correcting or deleting data); lessons learned and process improvements; or no further action where that is fair and reasonable on the evidence. We will communicate the outcome in writing without undue delay.

7. Instances when we may not take a complaint forward

We may decline, or take no further action, where a complaint is manifestly unfounded, excessive, vexatious or an abuse of process; the events are too old to investigate fairly; the same issue has already been addressed; a SAR has not yet been completed; there is no discernible breach or insufficient detail; identity or authority is not established. We will explain our reasons and remind you of your right to complain to the ICO.

8. Matters better dealt with elsewhere

Some concerns are better handled through another route. Where that is the case, we will explain why and where appropriate, forward the matter to the relevant team.

9. Reporting a data breach

If you believe your personal data may have been lost, wrongly disclosed, altered or accessed without authority, please also report it to dataprotection@rcsed.ac.uk as soon as possible, in addition to any complaint, so we can monitor and respond appropriately.

10. Independent external review (ICO)

If you remain dissatisfied after our process, you may refer the matter to the Information Commissioner's Office: Make a complaint | ICO, or by post to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. We will cooperate fully with any ICO enquiry.

11. How we use complaints data

We will record complaints and keep them in line with our Retention Schedules. We may use complaint data (in anonymised/aggregated form where possible) for reporting, evaluation, learning and service improvement and or monitor trends. We will only share personal data where there is a valid lawful basis (e.g. with staff handling the complaint, or with a regulator).

12. Roles, responsibilities and review

The CEO retains overall accountability for information governance. The Information Governance Group owns this procedure and has delegated day-to-day oversight of its implementation to the Governance, Risk and Compliance team.

All staff must recognise data protection complaints however they arrive and pass them to the Governance Risk and Compliance Team and cooperate with investigations.

This procedure will be reviewed at least every two years, with version control maintained.