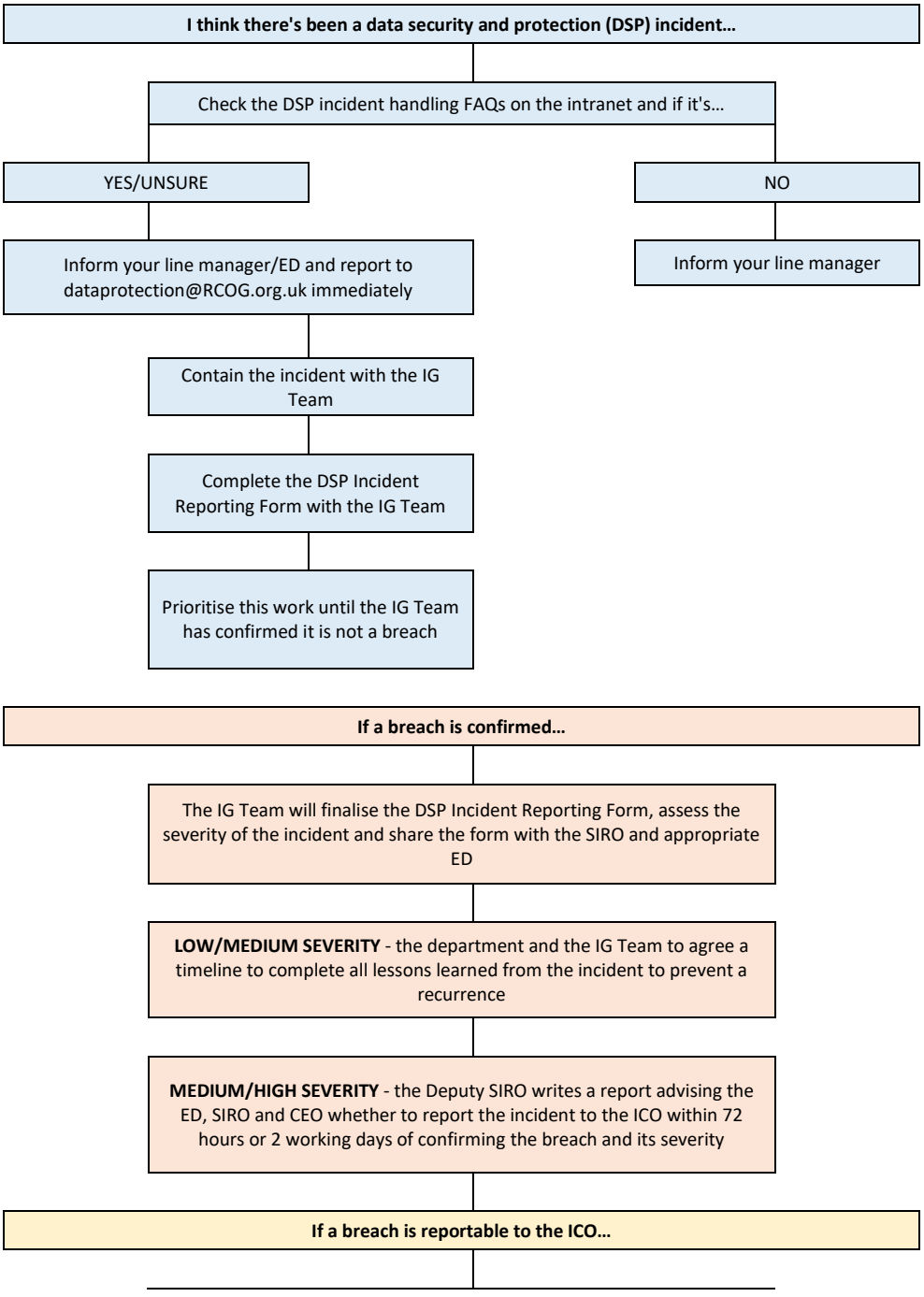
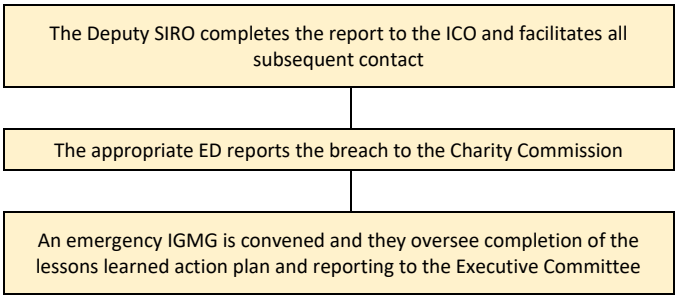
DATA SECURITY AND PROTECTION INCIDENT HANDLING POLICY AND PROCEDURES 2025

Working together to handle personal data safely, respectfully and lawfully

How to handle a data security and protection incident...





Contents

Introduction 3
Purpose 3
Scope 3
Policy 3
Governance 4
IGMG 4
Performance Monitoring 4
Roles and responsibilities 4
Definitions 5

Introduction

This Data Security and Protection Incident Handling Policy is the Royal College of Obstetricians and Gynaecologists' (RCOG or the College) policy regarding the swift and effective handling of all potential and actual data security and protection incidents, in line with the Information Commissioner Office's (ICO) guidance and RCOG Data Protection Policy.

Purpose

The purpose of the College Data Security and Protection Incident Handling Policy is to:

- assist you in the accurate identification of data security and protection incidents (the incident(s), suspected security weaknesses or near misses and security threats to services or systems
- advise you on how to report these incidents
- provide an outline of the investigation process
- empower you to be diligent and question procedures, protocols and events that you consider could cause damage, harm, distress, non-compliance or damage to the College's reputation, and
- enforce the College's Data Protection Policy.

Scope

The Data Security and Protection (DSP) Incident Reporting Policy and Procedure (the Policy) ensures the College is aware of what to do and who to contact in the instance of a potential or actual information security incident or data protection (DSP) breach occurs. This policy aligns with and flows from the Incident Response Policy and Guidance.

The Policy applies to **all employees (permanent, temporary, contracted and voluntary), officers, Board of Trustee/Committee members, trainees, members, College representatives and suppliers** who handle and use our information (where we're the 'Controller' for the personal data being processed), whether we hold it on our systems (manual and automated) or if others hold it on their systems for us.

Policy

The College commits to handling all Data Security and Protection Incidents in compliance with our Data Protection Policy, Incident Response Policy and Guidance and the Information Commissioner's Office (ICO) guidance.

ALL INCIDENTS TO BE TREATED AS HIGH SEVERITY AND OPEN UNTIL ASSESSED AS OTHERWISE AND CONFIRMED AS CONTAINED OR CLOSED BY THE IG TEAM AND/OR SENIOR INFORMATION RISK OFFICER (SIRO).

- Report all potential and/or actual data security and protection incidents immediately, ideally within 60 minutes to your line manager and the IG Team either by telephone or email where they:
    - EITHER, include RCOG Data Controlled personal data;
    - OR, 3rd party Data Controlled personal data
      Please note that if the 3rd party Data Controlled personal data contains patient data in any format then this notification is undertaken by the RCOG Caldicott Guardian
- Mark all emails relating to the incident with an IMPORTANT flag, and use the DSP incident reference number in the Title field form the point of allocation.

- Complete the Data Security and Protection Incident Reporting form in partnership with the Information Governance (IG) Team at: dataprotection@rcog.org.uk
- Provide as much detail as possible and be honest – many useful lessons can be learned from even the smallest of incidents
- All employees and third party, non-employees processing RCOG information must receive mandatory Information Governance Training within one month of joining the College. This training explains how to prevent, recognise and handle a data security and protection incident
- All employees involved with a data security and protection incident to receive classroom training delivered by either the Deputy SIRO or the IG Team
  All MEDIUM and HIGH SEVERITY incidents must agree and list proportionate Lessons Learned which are completed within 3 months of containing the incident with non-completion escalated to the Information Governance Management Group (IGMG). The lessons learned and action plan must be added to the local, relevant Standard Operating Procedure (SOP) to avoid a recurrence. Where an SOP does not exist then one needs to be created for the process/activity that resulted in the incident.
  - Data security and protection incidents caused deliberately or as a result of negligence may result in disciplinary action, as outlined in the staff Code of Conduct – e.g. knowingly transfer personal data without any protective controls without completion of a policy waiver form that records the issue, risk assessment and SRO sign off; or the posting of such information without consent or appropriate governance controls in place.

Governance

IGMG

The Information Governance Management Group (IGMG):

- Oversees the IG function of the College to ensure compliance is retained across the College
- Chaired by the SIRO
- Supported by the IG Team.

It is made-up of Directors from departments who process personal data and Subject Matter Experts (SME). All outstanding lessons learned and actions agreed by senior and executive management are escalated to these representatives who then take them back to their departmental/directorate management teams.

The terms of reference are included in the Data Protection Policy 2025.

Performance Monitoring

- IG Dashboards – RCOG performance against key statutory compliance requirements are monitored at least quarterly, covering:
  - Data Protection and Security Incidents – e.g. numbers logged as live, contained and closed with a severity rating and outstanding actions from lessons learned
- Audit and Risk Committee – quarterly compliance reports highlighting progress against regulatory (Data Security and Protection Toolkit) and statutory requirements using the IG Dashboards (see above), including anonymised summaries of incidents reported in that quarter.

Roles and responsibilities

- **All employees/handlers of RCOG personal data (see Scope)** to be alert to and report all potential DSP incidents as per this Policy.

- **Caldicott Guardian** notifies 3rd party Data Controllers subject to an incident occurring in partnership with the IG Team
- **IG Lead** to assist employees in the accurate identification of a DSP incident.
- **IGMG** to escalate outstanding actions form incidents at the quarterly meetings and review incident trends.
- **IG Team** to lead on all DSP incident investigations, consulting with and escalating to the Deputy SIRO as appropriate (part of the IG Team).
- **Relevant SLT and Line Management** to support their employees in handling a potential DSP incident by permitting them to prioritise it until the IG Team advise; and to notify their senior managers.
- **Deputy SIRO** to lead on HIGH severity incidents as per this policy and assist the IGO where appropriate (part of the IG Team).
- **Executive Committee** to work with the SIRO in deciding on whether HIGH severity incidents are reported onto the appropriate authorities, such as the ICO, Charity Commission and NHS Digital – all MEDIUM and HIGH severity incidents are reported to the relevant Executive Director and SIRO, with outstanding .
- **SIRO** to work with the Executive Committee in deciding whether HIGH severity incidents are reported onto the appropriate authorities, such as the ICO, Charity Commission and NHS Digital

Definitions

- **Data Security and Protection Incident:** includes, but not limited to, the loss, inappropriate disclosure, denial of access to, and destruction or erroneous modification of College information or information systems held both within RCOG systems and those held by third parties on our behalf.
- **Incident severity**:
    - HIGH
        - Particularly sensitive information at risk e.g. Clinical / Financial /Personally Identifiable
        - One or more previous incidents of a similar type in past 12 months
        - Failure to securely encrypt mobile technology or other obvious security failing
    - MEDIUM
        - Basic demographic data at risk e.g. equivalent to telephone directory
        - Limited clinical or financial information at risk
    - LOW
        - No clinical or financial data at risk
        - Limited demographic data at risk e.g. address not included, name not included.

For further advice concerning any aspect of this policy, please contact the Information Governance (IG) Team by email or call +44 20 7772 6309.