Data Security and Protection Incident Reporting Policy and Procedure

Working together to handle personal data safely, respectfully and lawfully

Scope
The Data Security and Protection Incident Reporting Policy and Procedure (the Policy) ensures the Royal College of Obstetricians and Gynaecologists (the College) are aware of what to do and who to contact in the instance an information incident occurs.

The Policy applies to:
- all staff (employed and contracted), officers, 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

Contents
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Contents</td>
<td>1</td>
</tr>
<tr>
<td>Objective</td>
<td>2</td>
</tr>
<tr>
<td>Policy</td>
<td>2</td>
</tr>
<tr>
<td>The Procedures</td>
<td>3</td>
</tr>
<tr>
<td>What is a Data Security and Protection incident?</td>
<td>4</td>
</tr>
<tr>
<td>What do I do if I cause or discover an incident?</td>
<td>4</td>
</tr>
<tr>
<td>Why do I need to report an incident to R&amp;IS?</td>
<td>5</td>
</tr>
<tr>
<td>How do I know if the incident is serious?</td>
<td>5</td>
</tr>
<tr>
<td>What happens in the event of a serious incident?</td>
<td>6</td>
</tr>
<tr>
<td>Our Incident Handling Toolkit</td>
<td>6</td>
</tr>
</tbody>
</table>
Objectives
The objectives of the Policy are 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 staff 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
- enforce the College’s Data Protection Policy.

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

- Report all data security and protection incidents within 24 hours or as soon as possible
- Complete the Data Security and Protection Incident form and send it to the Research and Information Services 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 staff involved with a data security and protection incident will receive classroom training delivered by either the Head of Information and Governance or the Information Governance Officer
- Data security and protection incidents caused deliberately or as a result of negligence may result in disciplinary action.
The Procedure

**Reporter**
Person experiencing or encountering the incident, also the person reporting it.

Reports the incident to the Research and Information Services Team within 24 hours or as soon as possible by completing a Data Security and Protection Incident form and sending it to dataprotection@rcog.org.uk. Also copying in the SIRO and the Information Asset owner usually the Director or IG Lead.

The Research and Information Services Team will request further information if required and assess the severity of the incident by using the Information Commissioner’s Office (ICO) “tests” to determine the severity and seriousness of the incident.

- Incident is reportable to the ICO.
- The “tests” determine if the incident is reportable to the ICO or not.

Incident is added to the register and reported to the ICO within 72 hours of it being assessed as a serious incident.

Next Steps:
- Notify data subjects
- Lessons Learned
- Data Security and Protection
- Incident training.

Incidents are reviewed at IGMG by the SIRO and closed when they have been mitigated effectively.

- Incident is not reportable.
- Incident is added to the register with the agreed mitigations and is monitored by IGMG.
What is a data security and protection incident?

A data security and protection incident is also commonly referred to as “a data protection breach”, “an information security incident”, and “a security incident”.

An incident includes, but is not limited to, the loss, inappropriate disclosure, denial of access to, and destruction or erroneous modification of College information or information systems.

It will or could result in:

- The disclosure of confidential information to an unauthorised individual – e.g. sending a fax to a wrong number, an email to the wrong recipient, a letter to the wrong address, using the general waste bin instead of the confidential waste bin
- The integrity of a system or data being put at risk – e.g. the loss or theft of equipment on which personal identifiable information is stored, writing passwords down and not storing them securely
- The availability of the system or information being put at risk – e.g. the theft of IT equipment
- Threat to personal safety or privacy – e.g. leaving confidential / sensitive files unsecured in a public area, loss or theft of confidential information held in paper records, failure to use the security measures provided such as secure email and protective marking (namely a failure to follow data protection policy) and using another user’s login ID or sharing passwords
- Legal obligation or penalty – e.g. unauthorised disclosure of information under contract and monetary fines as issued by the Information Commissioner’s Office (ICO)
- Financial loss – e.g. where personal data is lost or stolen and then used to commit fraud or crime
- Disruption of College business – e.g. hacking into College systems, download of malware through a phishing attack
- Reputational damage to the College – e.g. unauthorised disclosure of information for malicious intent.

What do I do if I cause or discover an incident?

Please:

- alert the Research and Information Services Team (R&IS) straight away, ideally within 24 hours of it happening
- complete the Data Security and Protection Incident form and send it to R&IS at dataprotection@rcog.org.uk
- copy in the Information Asset Owner (IAO), normally the Director or the IG Lead where the incident occurred, and the Senior Information Risk Officer (SIRO).

The R&IS Team then:

- review your completed form, requesting further information if required, and advise you of suitable containment actions to complete
- log the incident onto the data security and protection incidents reporting register, if it is not a near miss
- complete internal and Information Commissioner’s Office (ICO)”tests” to determine the severity and seriousness of the incident.
Why do I need to report an incident to R&IS?

All incidents logged on the register are reviewed and monitored by the Information Governance Management Group (IGMG) to identify recurring or high impact incidents. This may indicate the need for enhanced or additional controls.

Reporting incidents:

- allows the College to relate similar occurrences and highlight any areas of vulnerability, identifying where greater awareness is needed, and/or procedures/protocols require reviewing
- allows us to meet our legal obligation to report incidents to the Information Commissioners Office (ICO)
- provides reliable statistical data to keep the College informed.

It is important that data security and protection incident reports contain as much detail as possible. For example:

- a full description of the events and activities leading up to the incident
- information about the circumstances at the time of the incident, how it came about and how it was detected
- date, time and location of the incident
- the type of incident - e.g. loss of personal information, unauthorised access etc.
- the name and contact details of the person reporting the incident
- a detailed description of the incident - e.g. what happened - theft, accidental loss, inappropriate disclosure, procedural failure, etc.
- the type of record or data involved and its sensitivity – e.g. patient data, HR records, pseudonymised data, aggregated data with a value less than five
- the number (or estimate) of individual data subjects involved
- the number of records involved and the media (paper, electronic) of the records
- if electronic, whether the data was encrypted or not
- any other important factors necessary to determine the impact - e.g. local press involvement, incident reported by a member of the public, etc.

The report should be updated as more information becomes available, using the College’s advised version control to differentiate between updates.

R&IS’ initial assessment of the severity of the incident is entirely based on the reported facts, essential for them to provide sensible advice on the immediate, containment actions to be taken, including:

- recovery of the disclosed data (where possible) to limit the damage caused
- inform those who need to know
- assign responsibility and commence the investigation process.

How do I know if the incident is serious?

The College does not expect you to assess the seriousness of an incident. What may seem a small, insignificant incident to you could be happening across the College, indicating systemic failings in our processes – you cannot be expected to know this.

Therefore you must report all incidents to the R&IS following the above process.
What happens in the event of a serious incident?

If an incident is assessed as serious following the internal and ICO tests, the following steps are undertaken:

- the Head of Information and Governance produces an internal report for the SIRO and Chief Executive to decide whether to report to the ICO and notify the data subjects – the College has only 72 hours to report a serious incident, which is why it is essential to report all incidents to R&IS as a matter of urgency so we do not miss this deadline
- the Head of Information and Governance arranges an internal meeting with the key staff and officers involved to ensure the incident is contained, decide whether to notify the data subjects affected and agree a lessons learned action plan
- The IG Officer schedules Data Security and Protection Incident Breach training for all of the staff involved in the incident
- All incidents reported to the ICO are also reported to the Charity Commission.

Our Incident Handling Toolkit

The College has developed a toolkit to assist us in the handling of incidents – these are included in the appendices:

1. Data Security and Incident Examples and Types
2. Data Security and Protection Form
3. Data Subject Notification Template.

Another key ‘tool’ is staff training. All the staff and officers who have been involved in the cause, identification and investigation of an incident will receive classroom training.

<table>
<thead>
<tr>
<th>VERSION CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author:</strong></td>
</tr>
<tr>
<td><strong>Creation Date:</strong></td>
</tr>
<tr>
<td><strong>Signed off by:</strong></td>
</tr>
<tr>
<td><strong>Version:</strong></td>
</tr>
<tr>
<td><strong>Last review date:</strong></td>
</tr>
<tr>
<td><strong>Sign off Date:</strong></td>
</tr>
</tbody>
</table>

For further advice concerning any aspect of this policy, please contact Research and Information Services by email us or call +44 20 7772 6309.
### Appendix 1: Examples of Incidents and Incident Types

<table>
<thead>
<tr>
<th>Breach Type</th>
<th>Examples / incidents covered within this definition</th>
</tr>
</thead>
</table>
| **Lost in transit**     | The loss of data (usually in paper format, but may also include CD’s, tapes, DVD’s or portable media) whilst in transit from one business area to another location. May include data that is;  
- Lost by a courier;  
- Lost in the ‘general’ post (i.e. does not arrive at its intended destination);  
- Lost whilst on site but in situ between two separate premises/buildings or departments;  
- Lost whilst being hand delivered, whether that be by a member of the data controller’s staff or a third party acting on their behalf  
Generally speaking, ‘lost in transit’ would not include data taken home by a member of staff for the purpose of home working or similar (please see ‘lost or stolen hardware’ and ‘lost or stolen paperwork’ for more information). |
| **Lost or stolen hardware** | The loss of data contained on fixed or portable hardware. May include;  
- Lost or stolen laptops;  
- Hard-drives;  
- Pen-drives;  
- Servers;  
- Cameras;  
- Mobile phones containing personal data;  
- Desk-tops / other fixed electronic equipment;  
- Imaging equipment containing personal data;  
- Tablets;  
- Any other portable or fixed devices containing personal data;  
The loss or theft could take place on or off a data controller’s premises. For example the theft of a laptop from an employee’s home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk. |
| **Lost or stolen paperwork** | The loss of data held in paper format. Would include any paper work lost or stolen which could be classified as personal data (i.e. is part of a relevant filing system/accessible record). Examples would include;  
- letters;  
- employee records  
The loss or theft could take place on or off a data controller’s premises, so for example the theft of paperwork from an employee’s home or car or a loss whilst they were travelling on public transport would be included in this category.  
- Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system). |
| **Disclosed in Error**   | This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information itself hasn’t actually been accessed. Examples include: |
- Letters / correspondence / files sent to the incorrect individual;
- Verbal disclosures made in error
- Failure to redact personal data from documentation supplied to third parties;
- Inclusion of information relating to other data subjects in error;
- Emails or faxes sent to the incorrect individual or with the incorrect information attached;
- Failure to blind carbon copy (‘bcc’) emails;
- Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data;
- Disclosure of data to a third party contractor / data processor who is not entitled to receive it

**Uploaded to website in error**

This category is distinct from ‘disclosure in error’ as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include;
- Failures to carry out appropriate redactions;
- Uploading the incorrect documentation;
- The failure to remove hidden cells or pivot tables when uploading a spread-sheet;

**Non-secure Disposal – hardware**

The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include;
- Failure to meet the 6th Data Protection principle of the DPA 2018 and the security principle of GDPR for removal/destruction of data;
- Failure to securely wipe data ahead of destruction;
- Failure to securely destroy hardware to appropriate industry standards;
- Re-sale of equipment with personal data still intact / retrievable;
- The provision of hardware for recycling with the data still intact

**Non-secure Disposal – paperwork**

The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include;
- Failure to meet the 6th Data Protection principle of the DPA 2018 and the security principle of GDPR for removal/destruction of data;
- Failure to use confidential waste destruction facilities (including on site shredding);
- Data sent to landfill / recycling intact – (this would include refuse mix ups in which personal data is placed in the general waste)

**Technical security failing (including hacking)**

This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include:
- Failure to appropriately secure systems from inappropriate / malicious access;
- Failure to build website / access portals to appropriate technical standards;
- The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of industry best practice;
- Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces);
- Failure to implement appropriate controls for remote system access for employees (for example when working from home)
| **Corruption or inability to recover electronic data** | Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care/adverse clinical outcomes. For example:

- The corruption of a file which renders the data inaccessible;
- The inability to recover a file as its method / format of storage is obsolete;
- The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible |
| **Other** | This category is designed to capture incidents that do not fall into the aforementioned categories. These may include:

Failure to decommission a former premises of the data controller by removing the personal data present;

- The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data;
- Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets).

This category also covers all aspects of the remaining GDPR and data protection principles. |
<table>
<thead>
<tr>
<th><strong>Data Security and Protection Incident Reporting form</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Department Responsible:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Name of Reporter:</strong></td>
</tr>
<tr>
<td><strong>Date, time and location of incident:</strong></td>
</tr>
<tr>
<td><strong>The type of data involved, format and sensitivity:</strong></td>
</tr>
<tr>
<td><strong>Description of what happened:</strong></td>
</tr>
<tr>
<td><strong>Immediate action taken:</strong></td>
</tr>
<tr>
<td><strong>Lessons learnt (how will recurrence be prevented):</strong></td>
</tr>
<tr>
<td><strong>Internal Use</strong></td>
</tr>
<tr>
<td><strong>Incident Reference Number:</strong></td>
</tr>
<tr>
<td><strong>Incident logged in Security Incident Register</strong> (Y/N):</td>
</tr>
<tr>
<td><strong>SIRO informed (Y/N):</strong></td>
</tr>
<tr>
<td><strong>Does the Info Risk Register need updating (Y/N):</strong></td>
</tr>
<tr>
<td><strong>Does the President / CEO need to be informed(Y/N):</strong></td>
</tr>
<tr>
<td><strong>Incident closed (Y/N):</strong></td>
</tr>
</tbody>
</table>

**VERSION CONTROL**

<table>
<thead>
<tr>
<th>Author:</th>
<th>Version:</th>
<th>Creation Date:</th>
<th>Review date:</th>
<th>Signed off by:</th>
<th>Sign off Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IG Officer</td>
<td>Final</td>
<td>15 March 2019</td>
<td>22 March 2019</td>
<td>IGMG</td>
<td>29 March 2019</td>
</tr>
</tbody>
</table>