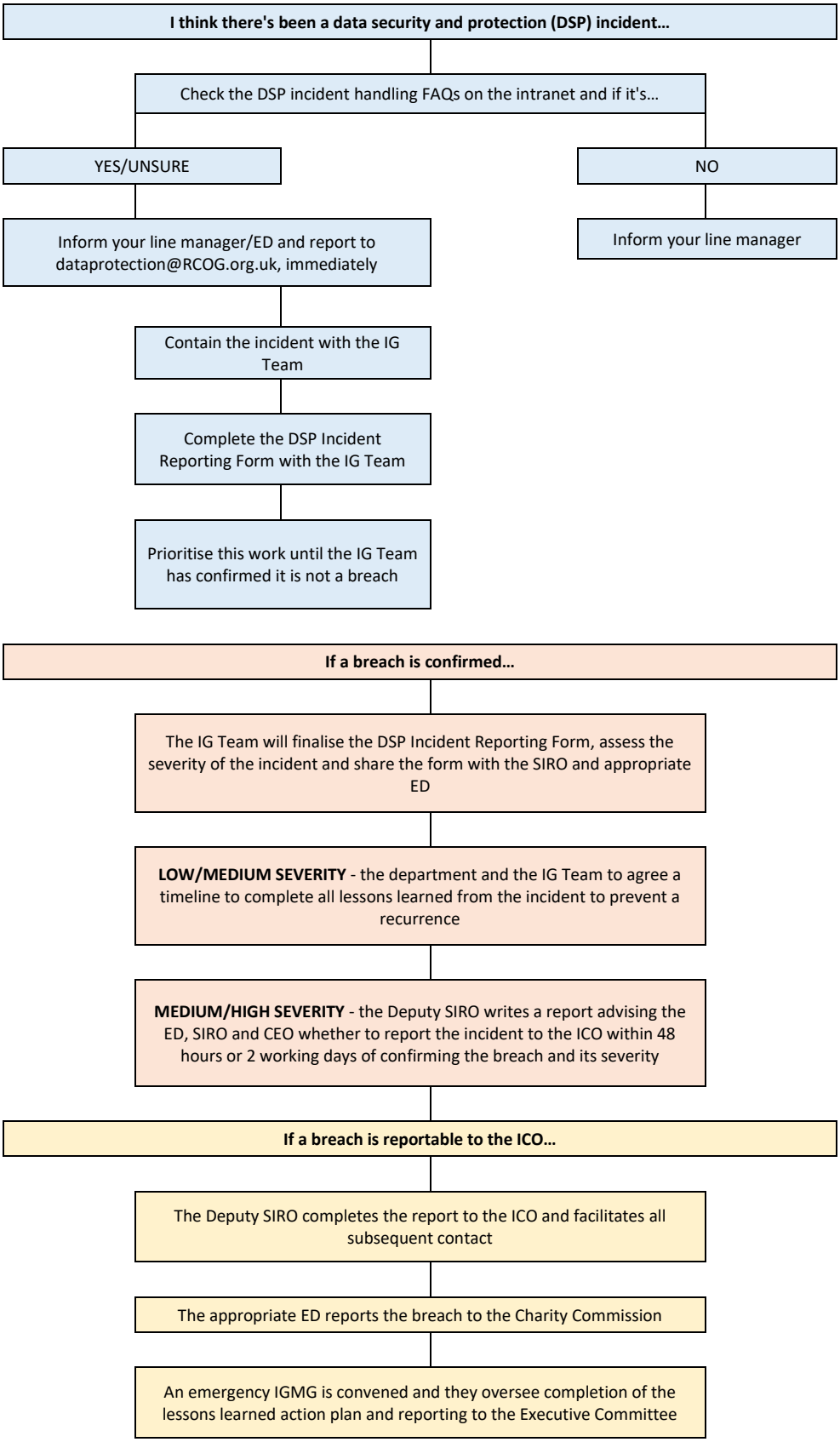
DATA SECURITY AND PROTECTION INCIDENT HANDLING POLICY AND PROCEDURE 2020

Working together to handle personal data safely, respectfully and lawfully

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



Scope

The Data Security and Protection (DSP) Incident Reporting Policy and Procedure (the Policy) ensures the Royal College of Obstetricians and Gynaecologists (RCOG or the College) are 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 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

How to handle a data security and protection incident... 1
Scope 2
Objectives 2
Roles and responsibilities 3
Definitions 3
Policy 3
Statement 3
Implementation 4
Our Incident Handling Toolkit 4
Appendices 5
Appendix 1: FAQs 5
What is a data security and protection incident? 5
What does an incident look like? 5
What do I do if I cause or discover an incident? 8
Why do I need to report an incident to R&IS? 8
How do I know if the incident is serious? 9
What happens in the event of a serious incident? 9
Appendix 2: DSP Incident Reporting Form 10
Appendix 3: Data Subject Notification Letter 11
Appendix 4: Deputy SIRO Advice Report 13

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.

Roles and responsibilities

- **All staff** to be alert to and report all potential DSP incidents as per this Policy.
- **IG Lead** to assist members of staff in the accurate identification of a DSP incident.
- **Information Governance Officer (IGO)** 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 members of staff 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.
- **SIRO** to work with the Executive Committee in deciding on 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.
- **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.

Policy

Statement

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 SIRO.

- Report all potential and/or actual data security and protection incidents within 5-60 minutes to your line manager and the IG Team either by telephone or email
- Complete the Data Security and Protection Incident form in partnership with the 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 staff involved with a data security and protection incident to receive classroom training delivered by either the Deputy SIRO or the Information Governance Officer

- All incidents must agree and list proportionate Lessons Learned which are completed within 3 months of containing the incident and monitored by the Information Governance Management Group (IGMG)
- Data security and protection incidents caused deliberately or as a result of negligence may result in disciplinary action.

Implementation

To comply with the Policy you must follow the Procedure below to the following timeline – to be developed into a SOP as part of the RCOG Incident Response Policy and Guidance :

FIRST 30 MINUTES	1. Establish the facts quickly: • Exactly when and how the information was disclosed/accessed • Confirm if the information contained personal data, referring to the College Data Protection Policy 2020: https://www.rcog.org.uk/en/about-us/policies/data-protection-policy/ 2. If yes, list the types of personal data, how much and the 3rd parties to whom it was disclosed or accessed by 3. Tell your line manager or IG Lead 4. Report to the IG Team on 020 7045 6790, 020 7772 6380, 020 7772 6309 or dataprotection@rcog.org.uk then work with them to agree and action immediate containment activities 5. The IG Team to log the incident and provide a reference number
FIRST 60 MINUTES	6. Following containment of the incident, work with the IG Team to complete the DSP Incident Handling Form 7. The first draft of the form will be shared with the Reporter of the incident, their Line Manager, their Executive Director and the SIRO
END OF FIRST WORKING DAY (within 24 hours wherever possible)	8. The IG Team to assess the severity of the incident, outline next steps/lessons learned and update the form 9. Next steps following incident assessment: • HIGH severity - the Deputy SIRO to convene an Incident Response Group meeting within the next 2 working days and draft an internal report for the relevant ED and SIRO • MEDIUM severity – next steps initiated, lessons learned agreed and initiated, including the team concerned to attend mandatory DSP Incident Handling Training • LOW severity – next steps completed and incident closed.

Our Incident Handling Toolkit

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

In summary:

- Mandatory training for the whole team affected by a HIGH or MEDIUM severity DSP incident
- FAQs
- Ref ##-DSP Incident Reporting-Form-V#
- Ref ##-DSP Incident-Data Subject notification letter-Template-YYYYMMDD
- Ref ##-DSP Incident-Deputy SIRO advice report-V#-YYYYMMDD.

For further advice concerning any aspect of this policy, please contact the Information Governance (IG) Team by email or call +44 20 7772 6200.

Appendices

Appendix 1: FAQs

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 does an incident look like?

Incident Type	**Examples / incidents covered within this definition**
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). In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate this risk.
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.

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 1 hour of it happening
- complete the Data Security and Protection Incident form in partnership with the IG Team an
- 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 IG Team will 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, including 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 IG Team following the above process.

What happens in the event of a serious incident?

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

- the Deputy SIRO produces an internal report for the SIRO and Executive Committee 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 the IG Team **as a matter of urgency** so we do not miss this deadline
- the Deputy SIRO 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 with MEDIUM or HIGH severity
- All incidents reported to the ICO are also reported to the Charity Commission and some may need to be reported to NHS Digital.

Appendix 2: DSP Incident Reporting Form

Department Responsible:	**Information Asset Owner/IG Lead informed (Y/N):** **Name of IAO/IG Lead:**
Name of Reporter:	**Contact details:** **Email: Tel:**
Date, time and location of incident:	
The type of data involved, format and sensitivity: •	
Description of what happened: •	
Immediate action taken: •	
Lessons Learned – to be completed within 3 months of containment: **1. …**	
INTERNAL USE ONLY	
Incident Reference Number:	
Severity: LOW/MEDIUM/HIGH	
Status: LIVE/CONTAINED/CLOSED	
Incident logged in Security Incident Register (Y/N): **SIRO informed (Y/N):**	
Does the Info Risk Register need updating (Y/N): **Does the President / CEO need to be informed(Y/N):**	**External/internal communication required (Y/N):** **Details if applicable:**
Incident closed (Y/N): N	**Date closed:**

Appendix 3: Data Subject Notification Letter

Dear [Title] [Surname],

Ref. ###: Data and Security Protection Breach of the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act 2018

It is with regret to inform you of a recent Data and Security Protection Breach concerning your personal data. This notification contains:

1. A summary of the breach
2. Our containment and immediate remediation actions
3. The potential impact on you
4. Summary of lessons learned
5. Your rights
6. Your responsibility [delete as appropriate].

The College takes your privacy seriously. We want to assure that we are taking this breach seriously and are committed to learning from this breach to avoid it recurring.

With this in mind we have informed the Information Commissioners Office (ICO) and will implement any recommendations we receive from them.

A summary of the breach
[insert here]

Our containment and immediate remediation actions
[insert here]

The potential impact on you
[insert here]

Summary of lessons learned
[insert here]

Your rights
As a data subject you have the right to request access to or challenge the processing of your personal data being held and managed by an organisation. Please see link to our website for further information on these rights and to access the individual rights request form: https://www.rcog.org.uk/en/about-us/policies/data-protection-policy/individual-rights-requests/

Your responsibility [delete as appropriate]
If you have had access to another's accidentally disclosed personal data that you were not expecting, please be advised that anyone who processes or shares this identifiable data with another individual are themselves breaching Section 170 of the Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/section/170/enacted - summary extracted below:

"170 Unlawful obtaining etc of personal data
(1) It is an offence for a person knowingly or recklessly—
(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained."

Please contact the College if you have any further queries or would like to make a complaint using the postal and email addresses above, or call us between 9:00am – 4:30pm (UK time) Monday to Friday on (+44)20 7772 6790.

If you are unhappy with how we have handled your personal data or responses to your queries, you can complain to the Information Commissioners Office (ICO). Please see the ICO website for details: https://ico.org.uk/make-a-complaint/your-personal-information-concerns; contact them directly by email to casework@ico.org.uk; or by post:

Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF.

Yours sincerely…

Appendix 4: Deputy SIRO Advice Report

1. Purpose of report

To provide Officers, the Executive Committee and Caldicott Guardian (where relevant) with Data Protection Officer equivalent advice following the reporting and investigation into a potential breach of the GDPR 2016 and/or Data Protection Act 2018.

A full chronology is contained within the DSP Incident Reporting form appended to this report. [Delete as appropriate]

2. Breach status: LIVE/CONTAINED/CLOSED **[Delete as appropriate]**

As of Day DD Month YYYY, this potential breach was logged by Research and Information Services (R&IS) with a status LIVE/CONTAINED/CLOSED [delete as appropriate] and a severity score of HIGH/MEDIUM/LOW [delete as appropriate].

HIGH *- Particularly sensitive information at risk. Failure to securely encrypt mobile technology or other obvious security failing e.g. involves Clinical / Financial /Personally Identifiable data, or one or more previous incidents of a similar type in past 12 months*

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.*

3. Notification to ICO: advice to Chief Executive, Executive Director(s), and Senior Information Risk Officer

SIRO Advice	
• ***Summary***: ○ … • ***Investigation outcome*** ○ 3-part test – outcome of R&IS' initial assessment which HoI&G will review and revise based on their view: 1. Did RCOG fail to have in place/take appropriate technical and organisational measures? Yes/No 2. Did a breach (i.e. loss, unauthorised access, corruption of data) occur? Yes/No 3. Has the breach had/will it pose a risk to the rights and freedoms of/cause damage and distress to the data subject(s)? Yes/No If all = Yes, then likely to need to report If all = No, then likely won't need to report If a mix of Yes and No, then will need further consideration by DPO as to advice on reporting to ICO ○ Complete ICO Self-Assessment - report a breach ○ Breach assessment grid – scored # (# impact x # harm) out of 25, equalling # ○ Notify data subjects – yes/no. • ***Advice***: ○ …	
Officer/CEO/SIRO Decision:	Accept/Decline

Reason for decision:	
Signature and job title:	
Date:	

4. Investigation chronology

Action	**Details**	**Time/Date**
Reported to the IG Team		
Potential breach confirmed		
Initial investigation started (2-4 working days)	•	
3 point test	1. Did the Controller fail to have in place/take appropriate technical and organisational measures? Yes/No 2. Did a breach (i.e. loss, unauthorised access, corruption of data) occur? Yes/No 3. Has the breach pose a risk to the rights and freedoms of the data subject(s)? Yes/No If all = Yes, then likely to need to report If all = No, then likely won't need to report If a mix of Yes and No then will need further consideration by SIRO/DPO as to advice on reporting to ICO – SIRO and Head of Information and Governance (HoI&G) advised to notify the ICO	
Breach assessment		
Actual breach confirmed		
72 ICO notification period started (3 working days)		
72 ICO notification period deadline (3 working days)		
SIRO/DPO advice confirmed and shared with Executive Management for a decision by the Chief Executive		

5. Related Incidents

RCOG reported incidents to the ICO:

- …

RCOG similar incidents not reported to the ICO:

- …

Recent ICO monetary penalties for similar incidents:

- # within the health or charity sector
- # across all sectors.

6. Potential breaches of the Data Protection Act 2018

A personal data breach is a security incident that has affected the confidentiality, integrity, or availability of personal data whenever:

- any personal data is lost, destroyed, corrupted, or disclosed
- if someone accesses the data or passes it on without proper authorisation
- if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

For example:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Therefore "... personal data must be processed in a manner that includes taking appropriate security measures about risks that arise from processing personal data" (Data Protection Act 2018).

7. Notification of Data Subjects:

…

8. Officers notified of the incident:

Officers

- …

Executive Committee:

- …

Departments

- Membership and Global – Ciara Shimidzu, Deputy SIRO/Head of Information and Governance
- Membership and Global – Forename Surname, Information Governance Officer.

9. Lessons learnt

a. …
b. …