Royal College of Occupational Therapists

Data Breach Policy

1. Introduction

This procedure is intended to be used when an incident of some kind has occurred that has resulted in, or is believed to have resulted in, a loss of personal data for which the Royal College of Occupational Therapists (RCOT) is a controller.

It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. If the 72-hour target is not met, reasons for the delay must be given and the organisation could be penalised for the delay.

Where an incident affects personal data, a decision must be taken regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2. Application of the policy

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the RCOT and its branches/specialist sections.

This policy applies to:

- All personal, special category (sensitive) data held or processed by the RCOT, regardless of format.
- All staff at the RCOT. This includes temporary, casual or agency staff and contractors, consultants, suppliers, volunteers and data processors working for, or on behalf of the RCOT.

3. Definition of Data Breach

For the purpose and context of this Policy, data security breaches include both confirmed and *suspected* incidents.

1.1 An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the RCOT's information assets and/or reputation.

1.2 An incident may include, but is not restricted to, the following:

- Loss or theft of personal or sensitive data or equipment on which personal data is stored (e.g. loss of laptop, mobile phone, USB, android or paper records)
- Equipment theft or failure
- Unauthorised use of, access to or modification of personal data or information systems
- Attempts to gain unauthorised access to information or IT systems
- Unauthorised disclosure of personal/sensitive data
- Hacking
- Environmental circumstances (e.g. fire)
- Human error

4. Reporting a Data Breach to the Data Protection Officer

There is an onus on all staff working for RCOT to report a suspected data breach to the Data Protection Officer as soon as possible, so that it is possible for the RCOT to meet the 72 hour window for breach notification (see section 5.1.2). The 72 hours applies irrespective of whether the breach occurs on a working day or a weekend and therefore the person who discovers the breach should report it asap even if it occurs on a non-working day.

Suspected breaches should be reported to:

Trevor White
Data Protection Officer (DPO)
Email: gdpr@rcot.co.uk
Telephone: 07384 258772

When reporting a breach to the DPO, please provide as much detail as possible about the breach, by completing the information required in section 1 of the Data Breach Notification form at Appendix A.

The DPO will make an immediate assessment about whether:

- Steps are required to contain the breach (see section 5.)
- The breach needs to be reported to the ICO (see section 5.1.1.)
- The data subjects affected need to be informed (see section 5.2.1.)

5. Containing and investigating the breach

Once the DPO has been alerted to a personal data breach, the DPO will need to understand whether the breach is still occurring or not. If the breach is still occurring or at risk of reoccurring immediately, then the DPO will need to identify what steps can be taken immediately to contain or stop the breach. This may require investigation and liaison with other members of staff, third party technology suppliers, processors or others.

The RCOT has a legal obligation to protect personal data it holds and therefore, it is paramount breaches are contained as quickly as possible.

Investigation will need to take place to understand what happened and what steps can be taken to mitigate the breach occurring again in the future. If the breach is required to be notified to the ICO, details of these steps will be included in the notification form.

6. Personal Data Breach Notification Procedure

Once it has been identified that a personal data breach has occurred, there are two parties who may be required by the GDPR to be informed. These are:

1. The supervisory authority
2. The data subjects affected

It is not a foregone conclusion that the breach must be notified; this depends upon an assessment of the risk that the breach represents to *"the rights and freedoms of natural persons" (GDPR Article 33)*. The following sections describe how this decision must be taken and what to do if notification is required.

6.1. The Supervisory Authority

The supervisory authority for the purposes of the GDPR for the RCOT is as follows:

Name:	Information Commissioner's Office
Address:	Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Telephone:	0303 123 1113
Email:	casework@ico.org.uk

6.1.1. Deciding whether to notify the Supervisory Authority

The GDPR states that a personal data breach shall be notified to the supervisory authority *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33).* This requires that the organisation assess the level of risk before deciding whether or not to notify.

Factors to be taken into account as part of this risk assessment should include:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The data types included e.g. name, address, bank details, biometrics and their sensitivity
- The volume of data involved
- The number of data subjects affected
- The nature of the breach e.g. theft, accidental destruction
- Any other factors that are deemed to be relevant

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Senior management
- Business area(s)
- Technology
- Information security
- Legal
- Data protection officer
- Other representatives as required

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by senior management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification
2. The personal data breach requires notification to the supervisory authority only
3. The personal data breach requires notification both to the supervisory authority and to the affected data subjects

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach. All decision making should be documented and saved as evidence.

6.1.2. How to notify the Supervisory Authority

In the event that a decision is made to notify the supervisory authority, the GDPR requires that this be done *"without undue delay and, where feasible, not less than 72 hours after having become aware of it" (GDPR Article 33).* If there are legitimate reasons for not having given the notification within the required timescale, these reasons must be given as part of the notification.

The notification should be given to the Supervisory Authority in section 5.1., by phone or online using the form Personal Data Breach Notification form. Please see: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ for more details on when to use each contact method.

The following information must be given as part of the notification:

a) The nature of the personal data breach, including, where possible:

i. Categories and approximate number of data subjects concerned

ii. Categories and approximate number of personal data records concerned

b) Name and contact details of the data protection officer or other contact point where more information may be obtained

c) A description of the likely consequences of the personal data breach

d) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

e) If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier

Written confirmation should be obtained from the supervisory authority that the personal data breach notification has been received, including the date and time at which it was received. Where necessary, the GDPR allows the information to be provided in phases without undue further delay.

Documentation of the personal data breach, including its effects and the remedial action taken, will need to be produced and can be captured in the ICO's Notification of Data Breach form.

6.2. Data Subjects

6.2.1. Deciding whether to notify data subjects

The GDPR states that a personal data breach shall be notified to the data subject *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34).* Note the addition of the word "high" over and above the definition given in Article 33.

The risk assessment carried out earlier in this procedure (section 5.1.1.) will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR.

Notification to affected data subjects is also not mandated by the GDPR where it *"would involve disproportionate effort" (GDPR Article 34).* However, in this case a form of public communication should be used instead.

Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

6.2.2. How to notify data subjects

Once it has been decided that the breach justifies communication to the data subjects affected, the GDPR requires that this be done without undue delay.

The communication to the affected data subjects *"shall describe in clear and plain language the nature of the personal data breach" (GDPR Article 34)* and must also cover:

a) Name and contact details of the data protection officer or other contact point where more information may be obtained

b) A description of the likely consequences of the personal data breach

c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

In addition to the points required by the GDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

In most cases it will be appropriate to notify affected data subjects via letter or email, or both, to ensure that the message has been received and that they have an opportunity to take any action required.

7. Annual review

This policy was approved by the Data Protection Officer on 25/06/2019. It will be reviewed annually by the Data Protection Officer to ensure that the purpose still applies.