GDPR2 – DATA BREACHES

1. INTRODUCTION

The General Data Protection Regulations/ Data Protection Act 2017(DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on SCMS who are responsible for processing it.

Anyone who processes personal data in SCMS is bound by the DPA.

Processing data means obtaining, recording and holding personal data and performing any operation on the data, including the erasure/destruction of the data.

Personal data is defined as information which relates to a living individual who can be identified from the data or from the data and other information which is in possession of, or is likely to come into the possession of, the data controller. The information may be in the either electronic or manual format.

Data protection breach is where data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully. Principle 7 states: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Information security measures are in place to protect personal data processed by SCMS staff and police officers, however a breach may occur from:

- Theft of data or equipment on which data is stored
- Loss of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Accidental Loss
- Destruction of personal data
- Damage to personal data
- Equipment failure
- Unlawful disclosure of personal data to a third party
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

GDPR2 – DATA BREACHES

2. REVISION AND APPROVAL

Rev.	Date	Nature of Changes	Approved By
1	01/05/2018	Original Issue	CEO
2	06/08/2023	Update	CEO
3	13/10/2025	Review and update paperless	CEO

3. SCOPE

This procedure applies to all potential and actual data breaches that occur during data processing controlled by SCMS staff.

4. PURPOSE

To meet the requirements of the Data Protection Act 1998, as amended, and the EU General Data Protection Regulations (GDPR) 2017.

5. RESPONSIBILITIES

Staff Member

- To report any potential or actual data breach immediately/asap to the Data Protection Officer(DPO)/Chief Executive Officer (CEO)
- To complete as many details of the potential or actual data breach on Form 955-Data Breach Report Form and pass it to the DPO/CEO
- To take immediate actions where possible to limit the effects of the breach prior to the DPO/CEO's assessment or actions

Chief Executive Officer (CEO)/Data Protection Officer (DPO)

- To review all reported potential or actual data breaches
- To onwardly report personal data breaches the meet the ICO's criteria to the ICO
- To undertake a risk assessment of the breach and put in place any actions to limit the impact

- To immediately report any personal data breaches to the individuals concerned and inform them of actions to be taken to limit their exposure caused by the breach.
- To onwardly report any breaches to any affected parties or stakeholders other than those relating to personal data breaches where required.
- To undertake a root cause analysis of the breach and instigate corrective and preventative measures to prevent a recurrence of the same event where possible.
- To complete Form 955- Data Breach Report Form and Form 956 – Data Breach Log with all details of the incident and resultant actions and outcomes.

6. PROCEDURE

6.1. If you discover that data has been lost, or if you believe there has been a breach of the data protection principles in the way that data is handled, you should immediately start to complete Form 955 – Data Breach Report Form with as many details as possible.

6.2. Pass the partially completed form to the Data Protection Officer (DPO)/Chief Executive Officer (CEO) no later than within 24 hours of first being aware/being notified of the breach.

6.3. Undertake any immediate actions possible to limit any further exposure whilst informing the DPO/CEO.
Comment: This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes, informing the police of a break in.

6.4. The DPO/CEO assign the breach a number by completing Form 956 – Data Breach Log with as many details as possible.

6.5. The DPO/CEO then follow the Information Commissioners Office (ICO) guidelines on notification and recording of the breach if this breach meets the criteria stated by the ICO.
Comment: Notification to the ICO is required within 72 hours and, if necessary, the DPO/CEO will inform the ICO by phone.

6.6. The DPO/CEO investigate and contain the situation as best as possible, consider who else may need to be notified and instigate a recovery plan including, damage limitation.
Comment: This may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

6.7. The DPO/CEO establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.
Comment: As well as the physical recovery of equipment, this could involve the use of backup tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

6.8. Where required the DPO/CEO will inform anyone whose data might have been compromised of the breach and explain what actions are planned to mitigate the breach both currently and to prevent further similar breaches.
Comment: Such communications may necessarily take place over a period of time to allow completion of the root cause analysis.

6.9. The DPO/CEO undertake a root cause analysis of the incident and complete the details of any actions on Form 955 – Data Breach Report Form including recommendations for updates on procedures, policies or forms.

6.10. The DPO/CEO ensure that all details on the Form and Log regarding the incident are completed and save an electronic copy of the complete Form in the Data Breaches Folder on the SCMS server.

7. RECORDS/REFERENCES

QS Form Ref.	Document Title
Form 955	Data Breach Report Form
Form 956	Data Breach Report Log

Log kept at: SCMS Docs Server/Data Protection/2 SCMS Data Breach and Subject Access Requests Log