SNAAP Data Breach Procedure

Last updated: 13 October 2025
Next review due: October 2027

---

1. Purpose

This procedure sets out how SNAAP will respond to any personal data breach, ensuring that we act quickly, minimise harm, and meet our legal obligations under the UK GDPR and Data Protection Act 2018.

A personal data breach is *any* incident that leads to the accidental or unlawful:

- loss,
- destruction,
- alteration,
- unauthorised disclosure of, or
- access to
  personal data.

---

2. Examples of data breaches

Data breaches can happen accidentally or deliberately. Examples include:

- Lost or stolen laptop, USB stick, or mobile phone containing personal data
- Email sent to the wrong recipient containing personal information
- Paper records lost, left unsecured, or disposed of incorrectly
- Database or system hacked or accessed without permission
- Personal data shared with an unauthorised person
- Information disclosed in error over the phone or via social media

---

3. Reporting a suspected breach

All staff, volunteers, and trustees must report any suspected or confirmed data breach immediately — even if unsure — to the Data Protection Lead:

📧 Carrie Wood, Manager – *carrie@snaap.org.uk*
📞 01227 367555

If the breach involves the Data Protection Lead, report it directly to the Chair of Trustees – Stephanie@snaap.org.uk

Do not try to hide or fix a breach yourself — quick and honest reporting helps us protect everyone's information and stay compliant.

---

4. Containment and recovery

Once a breach is reported:

1. Data Protection Lead logs the incident in the Data Breach Register.
2. Take immediate steps to contain the breach (e.g., recall emails, recover lost devices, change passwords, restrict system access).
3. Assess whether any data has been compromised or further risk remains.
4. Contact any relevant third parties (e.g., IT provider, payroll company) if their systems or data are affected.

---

5. Assessment and risk evaluation

The Data Protection Lead will assess:

- What type of data is involved
- How sensitive the data is (e.g., health, financial, safeguarding)
- How many individuals are affected
- Whether the data is encrypted or protected
- Likelihood and severity of risk to individuals' rights and freedoms (e.g., identity theft, distress, discrimination)

This risk assessment must be completed within 24 hours of the breach being reported.

---

6. Notification

If the breach is likely to result in a risk to individuals' rights and freedoms, SNAAP will:

- Notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach (via ico.org.uk).
- Record the justification if the breach is not reported to the ICO.

If the breach is likely to cause a high risk (for example, exposing sensitive information or identity theft risk), SNAAP will also:

- Inform the affected individuals as soon as possible, explaining what happened, what data was affected, and what they can do to protect themselves.

Trustees will be informed of all reportable breaches.

---

7. Record keeping

All breaches — whether reportable to the ICO or not — must be recorded in the Data Breach Register, including:

- Date and time of breach discovery
- Description of the breach
- Type and amount of personal data involved
- Number of people affected
- Actions taken and outcome
- Whether the ICO or individuals were notified
- Preventive measures introduced

Records must be retained for at least 6 years.

---

8. Review and prevention

After every breach (or near miss):

- Review what went wrong and how it happened.
- Identify lessons learned and update procedures or training.
- Reinforce data protection awareness across the team.

The Data Protection Lead will report significant breaches and learning points to the Board of Trustees at the next meeting.

---

9. Responsibilities

Role	Responsibilities
All staff and volunteers	Report breaches immediately and cooperate in containment actions.
Data Protection Lead	Lead breach response, notify ICO and individuals if required, maintain breach register, and report to Trustees.
Trustees	Oversee compliance and ensure this procedure is followed.