

Data Breach Response Policy

1. Purpose

This policy sets out how the charity identifies, reports, manages, and responds to data breaches. It supports compliance with UK GDPR, helps reduce harm to individuals and protects the charity's services, information and reputation.

2. Scope

This policy applies to:

- All trustees, employees, contractors, and third parties
- All systems, devices, and data managed or processed by the organisation
- Personal data, confidential business information and sensitive data

3. Definition of a Data Breach

A data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data. This includes incidents affecting the confidentiality, integrity or availability of personal data, confidential business information or other sensitive information.

Examples:

- Sending personal data to the wrong recipient
- Lost or stolen laptop containing data
- Cyberattack (e.g. ransomware or phishing compromise)

4. Roles and Responsibilities

All staff must report any suspected or actual data breach to help prevent further loss, disclosure or misuse of data.

- Immediately report suspected or actual breaches

IT Team

- Investigate and contain incidents
- Preserve evidence
- Support remediation

Data Protection Officer (DPO)

- Assess legal and regulatory requirements
- Determine notification obligations (e.g. ICO)

- Maintain breach records

Senior Management

- Approve major response actions
- Oversee communication and business continuity

5. Breach Identification and Reporting

All staff should report a suspected data breach as soon as they become aware of it. Staff should not wait to confirm whether an incident is a breach before reporting it. Early reporting allows the organisation to assess risk, contain the incident and meet any regulatory notification timescales.

5.1 Recognising a Data Protection Complaint

A data protection complaint is any expression of dissatisfaction about how the organisation has collected, used, shared, stored, protected, retained or otherwise handled someone's personal data. The person does not need to use the words "data protection complaint" for it to be treated as one.

Staff should recognise and escalate a possible data protection complaint where someone says, writes or suggests that:

- their personal information has been used, shared or disclosed incorrectly;
- information held about them is inaccurate, out of date, excessive or being kept for too long;
- they are unhappy with the response to a subject access request or another data protection rights request;
- they believe their personal data has not been kept secure or has been involved in a breach;
- they object to direct marketing, profiling, automated decision-making or another use of their personal data; or
- they want to complain about any matter involving the handling of their personal information.

Complaints may be received verbally, by email, letter, telephone, online form, social media or through routine contact with staff. If there is any doubt about whether a concern is a data protection complaint, staff should ask for clarification where appropriate and report it to the DPO for assessment.

The DPO will assess all reported data protection complaints and suspected or confirmed breaches and will decide whether, when, and how ICO needs to be notified. Staff must not contact the ICO directly about a breach or complaint unless instructed to do so by the DPO or senior management.

5.2 Immediate Reporting

All data breaches (suspected or confirmed) must be reported immediately to:

- IT Helpdesk Ticketing System
- Data Protection Officer (DPO)

5.3 Reporting Method

Include:

- Description of incident
- Type of data affected
- Number of individuals impacted (if known)
- Date/time of discovery
- Any actions already taken

6. Incident Response Procedure

6.1 Containment

- Isolate affected systems
- Disable compromised accounts
- Recover lost equipment where possible

6.2 Assessment

The assessment should establish what data was affected, type and sensitivity of data

- Volume of data affected
- Whether data was accessed or exfiltrated
- Potential harm to individuals

and what harm could result for affected individuals.

6.3 Risk Evaluation

The risk evaluation should consider the likelihood and severity of harm to affected individuals, including risks such as:

- Identity theft risk
- Financial loss
- Reputational damage
- Legal implications

6.4 Notification of authorities

The Data Protection Officer / IT lead and senior management should consider whether the incident must be notified to any relevant authorities, regulators, contractual partners or the Charity's cyber insurer.

Where the incident involves a cyberattack, ransomware, significant system compromise, business interruption, data loss or potential third-party claim, the Charity's cyber insurer should be notified promptly in line with the insurance policy requirements. Early notification helps ensure access to any approved incident

response support, legal advice, forensic investigation services and claims guidance available under the policy.

7. Notification Requirements

7.1 Regulatory Notification

A personal data breach must be reported to the Information Commissioner's Office (ICO) where it is likely to result in a risk to the rights and freedoms of individuals. The report must be made without undue delay and, where feasible, within 72 hours of the Charity becoming aware of the breach.

The 72-hour period starts when the Charity becomes aware of the breach, not when the investigation is complete. If all details are not yet available, an initial report should still be made and updated as further information becomes available.

- The DPO is responsible for assessing whether the breach meets the ICO reporting threshold and for submitting or coordinating the notification.

7.2 Individual Notification

Affected individuals must be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

- Where affected individuals must be notified, the Charity should provide the following information:
 - A clear description of the nature of the breach
 - The likely consequences for affected individuals
 - Steps the Charity has taken or will take to address the breach and reduce its impact
 - Recommended actions individuals can take to protect themselves, and contact details for further support

8. Communication Management

- Only authorised personnel may communicate externally about a breach. External communications should be coordinated with the Data Protection Officer, legal advisers where required, and the Communication and Engagement team to ensure that messages are accurate, consistent and appropriate.
- Maintain consistency in messaging
- Inform the Chief Executive who will inform the trustees.

9. Documentation and Record-Keeping

The Breach Register should record the incident details, investigation findings, risk assessment, decisions on notification, key timelines, actions taken, lessons learned, and any follow-up actions required.

- Incident details
- Investigation findings
- Actions taken
- Notification decisions and timelines

All personal data breaches must be documented, even where the breach does not meet the threshold for notification to the ICO or affected individuals. Records should show the facts of the breach, its effects, the risk assessment, the decision on whether notification was required, reasons for that decision, and the remedial action taken.

10. Post-Incident Review

After the breach has been contained and resolved, the Charity should complete a post-incident review of

- Conduct root cause analysis
- Identify control weaknesses
- Implement corrective actions
- Update policies and training as needed

11. Training and Awareness

- Yearly staff training on data protection and breach response
- Simulated incident exercises where appropriate

12. Policy Review

This policy should be reviewed at least annually and following any significant data breach, regulatory change, audit finding or material change to systems, processes, or organisational responsibilities.

- Annually
- After significant incidents or regulatory changes

13. Non-Compliance

Failure to comply with this policy may result in disciplinary action and legal consequences.