Data Breach Procedure

1. Purpose

This document outlines the procedure to be followed by all staff and volunteers of [Your Organization's Name] in the event of a suspected or actual personal data breach. This procedure is designed to ensure a prompt, effective, and compliant response, minimizing harm to individuals and the organization.

2. What is a Personal Data Breach?

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Examples include:

- Lost or stolen laptops, phones, or paper records containing personal data.
- Sending an email with personal data to the wrong person.
- Hacking or unauthorized access to an online database.
- Malware or ransomware attacks.

3. Immediate Actions (The "First Responder")

Any staff member or volunteer who suspects or discovers a data breach must:

- Do not panic.
- Immediately notify the Data Protection Lead: Contact [Name of Data Protection Lead/Role, e.g., "the Data Protection Officer" or "Operations Manager"] by phone or in person. Do not use email if the breach involves email security.
- Contain the breach: Take immediate, reasonable steps to stop the breach from spreading. This might include:
- Disconnecting a device from the network.
- Changing passwords.
- Shutting down a system.
- Retrieving a misdirected email.
- Do not inform others: Do not attempt to contact affected individuals or media yourself. All external communication will be managed by the Data Protection Lead.
- Secure the evidence: Make a note of the time, date, and details of the incident. This is crucial for the investigation.

4. Investigation and Assessment (The Data Protection Lead)

- Upon receiving a breach notification, the Data Protection Lead will:
- Log the breach: Record all details of the incident in a secure Data Breach Register.

- Investigate the breach: Determine the cause, scope, and nature of the breach, including:
- What personal data was affected?
- How many individuals are affected?
- What is the likely risk to those individuals (e.g., identity theft, financial loss, reputational damage)?
- Decide on next steps: Based on the risk assessment, the Data Protection Lead will determine the appropriate course of action.

5. Notification

- Notification to the Supervisory Authority (e.g., the ICO in the UK)
- The Data Protection Lead will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Notification to Affected Individuals
- The Data Protection Lead will notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- The notification will be clear and concise, explaining:
- The nature of the breach.
- The contact details of the Data Protection Lead.
- The likely consequences of the breach.
- The measures taken or proposed to be taken to address the breach.
- Any recommended steps the individuals should take to protect themselves.

6. Post-Breach Review

- Following a data breach, the Data Protection Lead will:
- Conduct a full review of the incident.
- Identify the root cause.
- Update security measures, policies, and procedures to prevent a similar breach from happening again.
- Provide additional training to staff and volunteers, if necessary.

7. Document Control

Policy Owner: [Name of Data Protection Lead/Role]

Last Review Date: [Date]

Next Review Date: [Date]