Data Breach Procedure

Definition: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes both accidental and deliberate events.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Responsibilities of Employees, Committee Members and Volunteers

All Employees, Committee Members and Volunteers will:

- Take steps to ensure the security of personal data at all times
- Know how to recognise a personal data breach
- **IMMEDIATELY** report any data breach of which they become aware to the Data Protection Officer/Data Protection Lead (DPO/DPL) Prompt action is essential, because reports to the Information Commissioner's Office must take place within 72 hours of the breach being discovered
- Record the nature of the breach and the action they have taken on a Data Breach Form

Responsibilities of the Data Protection Officer/Data Protection Lead (DPO/DPL)

Dealing with a personal data breach must be treated as an urgent priority and given adequate resources.

1. Assessment

- Assess the severity and likelihood of the potential adverse risks of the breach – see Appendix 1 'Level of Risk'. This assessment will include:
  - Nature of data involved
  - Sensitivity of data
  - Security mechanisms in place e.g. password protection
  - Information which could be conveyed to a third party about the individual
  - Number of individuals affected by the breach

2. External Reporting

- Based on the assessment, decide whether the breach requires external reporting to:
  - the Information Commissioner's Office (ICO). If it needs reporting, this must be done within 72 hours of the initial discovery of the breach even if full details are not yet known. Reasons must be given for any delay. Failure to notify the ICO when required to do so can result in a significant fine
  - the individual/s concerned: this must be done directly and without undue delay
  - Data processors for which the setting is a data controller
  - Data controllers for which the setting is a data processor

- Reports to the ICO must include:
  - A description of the nature of the personal data breach, including:
    - the categories and approximate number of individuals concerned
    - the categories and approximate number of personal data records concerned
  - The name and contact details of the setting's DPO/DPL
  - A description of the likely consequences of the personal data breach
  - A description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects

- Reports to individuals must be in clear and plain language and must include:
  - The name and contact details of the setting's DPO/DPL
  - A description of the likely consequences of the personal data breach
  - A description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects

- Reports to data processors and data controllers must be according to their contracts.

3. Containment and Action

- Decide what action needs to be taken to contain the breach and by whom
- Decide what action can be taken to recoup losses and/or limit damage caused by the breach
- Inform all relevant individuals of the action they need to take

4. Internal Investigation and Review

- Carry out an internal investigation into how the data breach occurred
- Determine whether the breach was a result of human error or a systemic issue
- Identify ways of preventing a recurrence e.g. through better processes or training
- Review and update processes as appropriate
- Review and update training and information for Employees, Volunteers and Trustees/Committee Members as appropriate

5. Recording and Internal Reporting

- Record full details of the breach, its effects and all decisions and action taken on a Data Breach Reporting Form
- Provide a written report on the breach to the Committee/Trustees/Senior Management

Responsibilities Of Trustees/Committee Members (for Charitable Settings)

- Individual Trustees/Committee Members have the same responsibilities as employees and volunteers, as stated above
- The Trustees/Committee Members are responsible for advising the DPO/DPL, for receiving and making reports on data breaches, and for reviewing the settings' response to data breaches

Appendix 1 - Level of Risk

Low: Low risk breaches may lead to possible inconvenience to those who need the data to do their job, such as the loss of, or inappropriate alteration of a telephone list. These should be dealt with internally but not reported to the ICO.

High: These are risks which may have adverse effects on individuals such as emotional distress and physical or material damage. They may include: Loss of control over personal data; Discrimination; Identity theft or fraud; Financial loss; Damage to reputation; Significant economic or social disadvantage.
These must be reported to the ICO.
These are examples taken from the ICO website. It is likely that guidance will become clearer over time.