VolunteerCentre Huntingdonshire

HVC Data Breach Policy

Signed .....

Review .....

Contents

1. **Background.** Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. The Huntingdon Volunteer Centre (HVC) needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2. **Aim.** The aim of this policy is to standardise the HVCs INITIAL response to any data breach and ensure that any breach is appropriately logged and managed in accordance with the law and best practice, so that:
   - incidents are reported swiftly and can be properly investigated
   - incidents are dealt with in a timely manner and normal operations restored
   - incidents are recorded and documented
   - the impact of the incident is understood, and action is taken to prevent further damage
   - the Information Commissioner's Office (ICO) and data subjects are informed as required in more serious cases
   - incidents are reviewed, and lessons learned.

3. **Definition.** Article 4 (12) of the General Data Protection Regulation ("GDPR") defines a data breach as: "a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed." HVC is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how HVC will initially manage a report of a suspected data security breach. The aim is to ensure that where a data breach as defined in the GDPR arises, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation. A data security breach can come in many forms, but the most common are as follows:

   - Loss or theft of paper or other hard copy
   - Data posted, e-mailed or faxed to the incorrect recipient
   - Loss or theft of equipment on which data is stored
   - Inappropriate sharing or dissemination - Anyone accessing information to which they are not entitled
   - Hacking, malware, data corruption

- Information is obtained by deception or "blagging"
- Equipment failure, fire or flood
- Non-secure disposal of data

4. **Reporting.** In any situation where volunteers or staff are uncertain whether an incident constitutes a breach of security or if there are IT issues, such as the security of the network being compromised, they should report it immediately to the HVC General Manager or Chairman of the Trustee Board.

5. **Scope.** This HVC policy applies to all HVC information, regardless of format, and is applicable to all staff, volunteers, contractors, partner organisations and data processors acting on behalf of HVC. The GDPR applies to all information users. All HVC Users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage. HVC management is responsible for ensuring that staff act in compliance with this policy and assist with investigations as required.

6. **Reporting a Breach.** All suspected data security breaches should be reported without due delay to HVC management via the Community Shop or Offices. The report must contain full and accurate details of the incident including who is reporting the incident and what data is involved. The incident report form should be completed as part of the reporting process. *See Appendix 1, Section 1.*

7. **Disciplinary**. Staff and volunteers who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

8. **Review**. This document shall be subject to annual review by the HVC TRUSTEE BOARD.

9. **References**

   The GDPR:- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG

   ICO GUIDANCE ON DATA BREACHES: https://ico.org.uk/

This policy was approved by the Trustees of Huntingdonshire Volunteer Centre

Signed: Mike Bates *Chairman*

Date: 5th August 2025

Date of next Review: