Data Breach Policy

Requirement

We are required to report personal data breaches.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data[1] is lost, destroyed, corrupted or disclosed; If someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant effect on individuals.

Examples include access by an unauthorised third party; deliberate or accidental action (or inaction) by a member of staff, sending personal data to an incorrect recipient; and a computer containing personal data being lost or stolen.

Reporting

We need to tell the Information Commissioner's Office within 72 hours if it is likely there is a risk to people's rights and freedoms (i.e. more than just inconveniencing them)

We need to tell individuals directly if the breach has a high risk to their rights and freedoms without delay.

We need to keep a record of all breaches, even if not reportable to the ICO or individuals.

Reporting procedure

- Any data breaches of personal data by CCCW staff and Henry Martyn Trustees should be reported immediately to the HMT Chair and CCCW Administrator.
- Those informed will decide whom to notify. Consideration will be given to notifying the ICO and the individual(s) whose data is affected.

Reports will be made in accordance with the ICO regulations at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches or as subsequently updated.

[1] Personal data is defined as any information that can identify a living individual