## Introduction

West Wiltshire and East Somerset Area Meeting (WWESAM) collects, holds, processes, and shares personal data that needs to be suitably protected. Every care must be taken to protect personal data from incidents or breaches (either accidentally or deliberately), which may result in harm to individual(s),and the Area Meeting.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents. It relates to all personal data held by the Area Meeting, regardless of format. The objective is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches. It applies to data security breaches both confirmed and suspected.

An incident includes, but is not restricted to,

1. the loss or theft of confidential or sensitive data or equipment on which such data is stored e.g. loss of laptop, USB stick, iPad / tablet device, or paper record.
2. Unauthorised use of, access to or modification of data or information systems; or attempts at these (for example, hacking attack on IT system).
3. unauthorised disclosure of sensitive / confidential data;
4. unforeseen circumstances such as a fire or flood, human error leading to an incident.

## Reporting an incident

Any individual who accesses, uses or manages information on behalf of WWESAM is responsible for reporting data breach and information security incidents immediately to the Clerk to Trustees. This should be done by fully completing an Incident Report Form (see page 3 below).

## Containment and recovery

The Clerk to Trustees will determine the appropriate steps to minimise the effect of the breach, recover any losses, and limit the damage the breach could cause. The clerk will inform the police, insurers and banks, where appropriate. Wherever possible, this should be done within 24 hours of the breach being discovered and reported.

The Clerk to Trustees will then investigate further, for example examining adverse consequences for individuals, how serious or substantial those are, and how likely they

are to occur. This must include considering the type of data involved, its sensitivity, the protections that are in place (e.g. encryptions), what has happened to the data (e.g. has it been lost or stolen), whether the data could be put to any illegal or inappropriate use; the data subject(s) affected by the breach, number of individuals involved and the potential wider consequences.

## Notification

The Clerk to Trustees will, in consultation with other Trustees, establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. In doing this the Trustees accept that not every incident warrants notification and will seek the advice of Friends House where appropriate.

Where an incident is deemed likely to bring a high risk of adverse effect to an individual's rights and freedoms, those individuals will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

A record will be kept of any personal data breach, regardless of whether notification was required, and recorded in the minutes of Trustee meetings.

## Evaluation and response

Trustees will carry out a review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken to minimise the risk of similar incidents occurring.

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

# Data breach report form

Please act promptly to report any data breaches. If you discover a data breach, please notify the Clerk to Trustees.

Date incident was discovered: _____ Date(s) of incident:_____

Place of incident: _____

Name of person reporting incident: _____

address or email address: _____

telephone no: _____

Brief description of incident or details of the information lost:

Number of Data Subjects affected, if known: _____

Has any personal data been placed at risk? If, so please provide details:

Brief description of any action taken at the time of discovery:

For use by Clerk to Trustees (name: _____)

Date received: _____

Assessment of incident (must include an assessment of severity):

For further information and guidance on handling data breaches, please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

| | | |
|---|---|---|
| Issued | 1 July 2018 | *West Wiltshire and East Somerset Area Meeting of the Religious Society of Friends* |
| Adopted by AM | | |
| Revised | 15 July 2018 | |