PD3b Personal Data Breach Handling and Notification Policy

1) Introduction

This policy describes the steps that are to be taken whenever it is known, or suspected, that personal data security may have been breached.

2) What is a personal Data Breach?

A personal data breach has taken place whenever the following happens to some personal data controlled by the U3A.

- It has been lost, corrupted or destroyed
- It has been, or may have been, accessed by unauthorised persons
- It has been disclosed or altered without authorisation
- It has been used for purposes other than those for which it was provided

Examples of potential breaches include

- A laptop containing a list of members is lost or stolen
- A USB drive containing personal data is stolen
- A note book containing a written list of group members is left in a public place
- Beacon is hacked and the database accessed
- The membership database is lost, and backups cannot be restored
- A group coordinator provides a list of group members to an outside organisation without specific consent

3) How are we notified of a Data Breach?

In many cases it will be the person handling the data who becomes aware of the breach, or potential breach. However, in some cases the notification will come from outside the committee or even from outside the U3A. In this case the person raising the concern should, if they contacted us by phone, be asked to contact us again in writing, either by email or by letter, giving as much detail as possible. Depending on the seriousness of the allegation it may be necessary to act without waiting for the written statement to arrive.

4) Who Should be Notified?

All reports of breaches should be notified to the chairman of the U3A within 24 hours. Upon receiving a notification the chairman should start the following process as soon as practical. He/she would be expected to call upon the help of any suitable committee member who is be able to help, but the chairman must maintain overall control of the situation.

5) Breach Handling Process

The breach handling process is as follows.

The very first thing to do is to decide whether the allegation is credible. If the person reporting the breach is a committee member or group coordinator then there will be an assumption that the report is genuine. If the report comes from elsewhere a very rapid (same working day) assessment must be undertaken to eliminate obviously spurious notifications. If the notification fails the assessment then the person who notified us will be told of the outcome of our investigations.

In any case the committee must be informed that a breach has, or may have, occurred, and they should be told the nature of the breach. Members of the committee are all trustees, so share responsibility.

Assuming that the breach notification has not been rejected, the first priority is rectification and damage limitation. If the cause of the breach is obvious and can be resolved, then this step is easy. If ongoing and/or not easy to solve, for example somebody gaining access to BS U3A's Beacon via an unknown route, then it may be necessary to take the service down until the source of the problem has been identified and corrected.

At a very early stage an assessment must be made of:

- Whose personal data has been compromised?
- How damaging could this breach be to them?

The chairman must contact the Third Age Trust within 24 hours and discuss the breach with them. They will advise on matters such as actions to be taken, and whether the Information Commissioner needs to be informed. However, the final decision to report the matter or not must be made by the chairman of BS U3A and not a member of another organisation.

If a breach has been found to have occurred then it must be reported to the Information Commissioner within 72 hours – and no allowances are made for holidays or weekends.

6) Informing the Members Concerned

Any member whose personal data has been affected by a breach should be notified. The notification should tell them what has happened and what we are doing to remedy the situation. They should also be informed that they have the right to contact the Third Age Trust if they are unhappy at our handing of the situation, and ultimately they can complain the Information Commissioner's Office.

7) Record Keeping

A file of all decisions, with reasoning, should be kept of each breach or suspicion of a breach by the chairman.