Data Protection and Security

DATA PROTECTION GUIDANCE

PERSONAL DATA AND SENSITIVE PERSONAL DATA

Personal data means any data which relates to an individual who can be identified from this data (with or without other additional information): For example, names, email addresses, telephone numbers and addresses are all personal data. Personal data of this type should be the only type of data included in the U3A membership databases. No other type of information or data should be included.

Personal data also includes any expression of opinion about that individual and any indication of the intentions of a University of the Third Age organisation (each a "U3A") or any other person in relation to that individual. This sort of personal data should not be collected in a U3A membership database

Sensitive personal data means personal data consisting of information as to:

- the racial or ethnic origin of the individual.
- political opinions.
- religious beliefs or other beliefs of a similar nature.
- whether he/she is a member of a trade union.
- physical or mental health or condition.
- sexual life.
- the commission or alleged commission of any offence.
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

DATA PROTECTION PRINCIPLES

Under current Data Protection law, a U3A must comply with the following 8 data protection principles.

1. Personal data shall be processed fairly and lawfully.

- Processing is broadly defined and in effect will cover any activity involving personal data (such as obtaining, recording, holding, using, disclosing or erasing data). This principle will usually be met if the individual is informed of the fact that the U3A intends to process personal data and what the U3A intends to do with it. i.e the

members consent to be on a database to allow the U3A to contact members about U3A activities of a local, regional or national nature
- Consent to keep records is not strictly necessary for personal data, but is recommended.
- Before processing sensitive personal data about an individual (for example, entering it on a database), ensure that you have obtained the individual's explicit written consent It is not anticipated that the collection of sensitive data will ever be required by a U3A membership database
- If you receive data from a 3rd party, please check with that 3rd party that consent was received from the data subject (the person to whom the data relate to) before those were sent out externally.

2. Personal data can only be obtained for the purposes specified to the individual, and cannot be processed in any manner incompatible with those purposes.

- Only use personal data in a way that falls within an individual's reasonable expectations or stated purposes.
- If you are going to use the information for any purpose that goes beyond this, such as to add names to a marketing list and/or pass on the data to a 3rd party, you must explain this clearly and obtain their specific consent from each member on the database before passing data to third parties .
- Do not send e-mails or SMS for marketing purposes without getting consent from the intended recipient.
- If a person indicates that they do not want to receive marketing communications, amend the relevant database and ensure that the person's wishes are respected by notifying all internal contacts who need to know.
- Before transferring personal data outside the U3A, ensure you have obtained the individual's consent.

3. The collection of personal data has to be adequate, relevant and not excessive compared to the purpose(s) data is collected for.

- Collect only personal data that is necessary for the purpose in hand e.g. names, email addresses, telephone numbers and addresses. Do not collect irrelevant or excessive personal data.
- When collecting information on a database, drop-down boxes and free-text boxes need to be examined carefully to avoid unnecessary personal data and sensitive personal data being collected.
- Do not enter negative comments on any individual, including U3A members or suppliers, onto any database.

4. Personal data held should be accurate and, where necessary, kept up to date.

- Regularly check what records are kept, and make sure you are not keeping information that is irrelevant, excessive or out of date.

5. Personal data processed for any purpose(s) cannot be kept for longer than is necessary for the purpose(s).

- Delete information that you have no genuine business need for. As a rule of thumb, personal data about a U3A member who has left the U3A should be deleted within 6 months.
- If you need to hold data for longer than what is really necessary, hold the data in an anonymised way.
- Ensure that records which are to be disposed of are securely and effectively destroyed.

6. Personal data has be processed in accordance with the rights of data subjects.

- Data subjects (individuals or companies) have a legal right of access to information the U3A holds on them. They can find that out by sending the U3A a request for information or "data access request". If you receive such a request, please forward it promptly to the Business Secretary in your U3A, and advise the Business Secretary to contact National Office for assistance.

7. Appropriate technical IT and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Keep personal data and sensitive personal data secure (for example, keep records in a locked cabinet, use password protection and restrict access to specific U3A Executive Committee members– please see the Information Security document for more information).
- Ensure that all members comply with the below Data Security Checklist.
- If a 3rd party supplier is engaged to do any of the processing on behalf of the U3A, ensure a legal review of the contract with that supplier is undertaken. This needs to ensure that the supplier agrees to act only on the U3A's instructions and to comply with specified security measures.

8. Personal data cannot be transferred to a country or territory outside the European Economic Area unless that country or territory ensures

an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Always talk to National Office who will obtain advice if you intend to transfer any personal data outside of the EEA.

DATA SECURITY AND E-EMAILS CHECKLIST

- If you use a password, ensure that you use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.
- Always keep your password and user name secure and do not share them.
- Always lock your PC while it is unattended.
- Consider sending confidential information by secure e-mail.
- Do not open e-mail attachments from an unknown source.
- Do not to open spam – do not even unsubscribe or ask for no more mailings. Instead delete the email and either get spam filters on your computers or use an email provider that offers this service.
- Do not to believe emails that appear to come from a bank that ask for account, credit card or password details (a bank would never ask for this information in this way).
- Avoid asking for sensitive personal data unless necessary for a legal or business purpose, or passing on sensitive personal data about somebody else.
- Do not make negative comments about any individual, including other U3A members or suppliers. If you feel that there is an issue which other people need to be aware of speak to National Office first about the next steps.
- Do not send any e-mail which might be construed as offensive or discriminatory and do not download obscene material.
- Do not download programmes or games, or run any such programmes or games sent to you by e-mail.
- Do not download business data onto any personal laptop unless authorised.
- Ensure that any personal data held on a laptop is encrypted.
- Tidy your inbox, outbox and folders regularly. Do not store messages or attachments longer than necessary.
- When taking records or laptops off-site, ensure that: (i) only the necessary information is taken; (ii) such information is controlled at all times; and (iii) U3A security advice is followed.
- If your laptop is lost or stolen, contact National Office immediately.