Good Practice for Handling Data

Background

Our organisation intends to conform to the **General Data Protection Regulation (GDPR)**, effective from May 2018. A Data Privacy Notice (which includes our policy) will be published. All organisations, and every single person running them, should be aware that they are responsible for keeping data safe and for not keeping it longer than necessary. We should avoid giving criminals any opportunity to collect and connect scraps of personal data. Equally, we should duplicate and back up so that records are not lost in the event of fire, flood, computer breakdown or theft.

Data Included

Personal data means not just names and addresses, etc., but also information about a person which is potentially sensitive or embarrassing to that person and to us. Financial data is included where it is commercially sensitive (such as quotations for work or prices paid) but need not be included where it is in the public domain, such as annual accounts.

Paper Records

- Store paper records in your locked house (when you are out), out of sight in a file or drawer.
- Do not circulate more copies than needed.
- Keep lists and rotas out of sight. When they must be posted on a board, show names only and not addresses, telephone numbers or email addresses.
- Destroy records by shredding or burning.

Records on Computer

- Set up your computer with an account password so that you have to log in every time you use it.
- If there is no account password (as above), protect any digital files containing personal, sensitive or confidential data with a password. Consider protecting some files anyway.
- For the sake of 'business continuity', write down instructions and the passwords and seal them in an envelope. Give that envelope to a trusted person so that he or she would be able to access important files in the event of your incapacitation. In addition, give either the same details or the name of the trusted person to the organisation's Controller. Alternatively set up a secure cloud storage and sharing service (for example Dropbox).
- Backup your digital files using some medium other than the host device: for example external hard drive, CD or flash drive. The backups should ideally be kept well away from your computer so that both would not be destroyed in a fire. Alternatively backup to secure cloud storage. Backup at least weekly and preferably daily.
- When you delete a file, it is hidden from view: it is not actually destroyed. This means that anyone with a little knowledge can easily recover the file. Even formatting a disk does not actually destroy data. So when you sell or dump a computer or any storage device, it is vital that you protect the data. You can securely overwrite the data with a free application called 'Eraser' from Heidi Computers (or there are many others). You can securely overwrite free space (where old files reside out of sight) at any time with, for example, the free application 'CCleaner'. Or you can physically remove the hard drive and smash it comprehensively.
- In any case, destroy old records on your computer by securely overwriting them.

Daily Practice

- Keep your anti-virus up to date on your computer.
- If you believe your computer has been scammed, lost or stolen tell the others in our organisation so that risk of data theft can be assessed. *[Action Fraud: actionfraud.police.uk or 0300 123 2040].* Some data breaches, for example identity theft, must be notified to the ICO within 72 hours.
- Never send mass emails with the names of recipients visible in the 'to' or cc field. Use bcc (blind carbon copy).
- Avoid printing out when it is not necessary.
- Avoid too many copy addressees on paper and on computer.

Permission and Data Protection Notices

- Under the GDPR, the information in our Data Privacy Notice should have been seen by anyone you are keeping data about, but explicit consent is not needed for everyday admin.
- An application form can conveniently include consent specific to it. The notice should say something like: 'Your personal data will be treated as strictly confidential and will only be shared, when necessary for administration, with other members of the Committee. We will only share your data with third parties with your consent. Our full Data Privacy Notice can be seen at the Secretary's office'.
- Consent in the above example does not give consent to other data processing, such as writing a begging letter. However, there is also a consent form which covers everything.
- Consent forms, where needed, must be kept (by the Secretary).
- When sending for example, a newsletter, always add a note that the recipient may unsubscribe at any time.

Retention and Disposal. We keep data, specifically email addresses of local people who wish to be kept informed of events and Committee Members' contact details while it is still current; financial data and associated paperwork for up to 7 years after the tax year for which they are still valid; and details of contractors and insurance permanently.
Otherwise we securely dispose of material when it is no longer applicable or needed, or is more than 7 years old **with the exception of**:
Historical or very interesting material; minutes of meetings; evidence of title, boundaries and maps; policy decisions; proof of insurance, which should be kept indefinitely against a long-term claim; one copy of the annual accounts.
These excepted items should be carefully kept in a dry place.

Associated documents
Data audit
Data Privacy Notice (which also shows where consent is needed, see para 'Legal Basis').
Consent Form

March 2018
Sponsor: Secretary