British Sundial Society Computer Data Backup and Disaster Recovery Policy

Applicability

Members and Specialists are individually responsible for the security of all Society data under their control. This Policy is recommended for use by all members of the BSS Council and all others such as our Specialists who use computers in any way for Society business.

Introduction

Increasingly the activities of the Society are being developed and recorded by using computers. The volatility of the main memory, the fragility of hard disc storage of any computer and the limited life even of data offloaded to CD or DVD means that all who use computers for and on behalf of the Society must take steps to minimise the risks of data loss and additionally to provide for the easy and reliable transfer of their data files to other systems.

The Risks

This policy is designed to provide guidance on ways by which the following risks may be contained and operation continued.

- Inadvertent deletion or overwriting of data by the User
- Physical failure of the hard drive within the computer being used
- Failure of the computer itself – perhaps by an electrical surge or by a house fire
- Theft or vandalism of the computer and of local data storage and files kept nearby
- The need for others to take over, use and thereafter control, your files

Actions to be taken by all Council members

1. Where at all possible, adhere to the Society's policy for using PCs rather than Macs and for the use of Microsoft and Adobe Software as far as possible. This ensures that all computer data may be more readily read by all across the Society and where necessary be operated by others on other PCs.

2. Set up a series of designated folders into which all Society information will be kept. This ensures that all Society data is kept together in an easily accessible form.

3. Provide an environment where backup of data may be made to a hard drive that is wholly independent from the hard drive used by the operating system. This may be easily achieved by the one off purchase of an external USB-connected hard drive of adequate capacity. The Maxtor One Touch 4 is one such and is available (in 2009) at around £60.

There are also some web based backup facilities like that available at http://www.backuptotheweb.net which may be may be used at a cost (in 2009) of around £60/year for 5GB storage. Web based backup facilities utilise the professional services of large companies and so normally represent a high level of security. However they usually will require the availability of a broadband connexion on the PC and of course they represent an ongoing cost to the Society which will need the prior approval of the Treasurer.

In some very important situations like the Society's accounting files it may be prudent to employ both an external USB hard drive and web based back up facilities.

- *These approaches to backup ensure that failure of the main hard drive of the PC cannot result in the loss of the backed up data.*

[Note that some PCs use a single physical hard disc which is partitioned to give the impression of two or more logical hard drives. Those 'logical' drives are not suitable for use as a backup medium since physical failure of the hard drive will also result in loss of all such 'drives'.]

4. Set up an automated process by which all Society folders and all other important computer data are backed up every day to the physically separate external hard drive. If choosing web based backup ensure that it will perform automatic scheduled back ups so that you do not have to remember when to make a backup.

Scheduled backups to an external hard drive can most sensibly be performed by the one off purchase of the award winning program "Second Copy".
This may be purchased at http://www.SecondCopy.com and its purchase is a valid and claimable Society expense. It provides for the automatic backup of files from designated folders and, set up properly, it will even retain several past copies so that even if some data comes to be deleted or overwritten by mistake by the User and the fact is not realised for some days the original data may still be recovered.

It is probably best to set up *Second Copy* so that the backup files are not overwritten by the content of the latest versions on the main hard drive when next they come to be backed up. This gives greatest security and also gives access to past versions of the files but it does result in an ever increasing amount of data being stored on the USB Backup drive.

- *When properly used, this approach ensures that locally backed up data can never be more than one day out of date.*

5. At monthly intervals copy to DVD all backup data stored on the USB hard drive. Use a write-once DVD such as DVD-R. Do not use any form of re-recordable media. After recording ensure that the disc is finalised to allow the DVD to be read on other PCs and verify that after writing the DVD can indeed be read back. Keep as many of these backup discs as may be necessary and for as long as necessary to protect the Society's business. This may be a few months for something like the Register or for one or more years for something like the Society's correspondence or finances.

If the chosen process of backup using Second Copy does result in an ever increasing content on the external backup hard drive then after a successful complete back up to DVD (and subsequent verification) the contents of the external hard drive may be deleted and a new backup process allowed to start when Second Copy next resumes.

- *This approach ensures that even if the computer and the external hard drive fail or comes to be stolen or vandalised only one month's data might be lost.*

6. At six monthly intervals send a DVD write-once backup copy of the external backup hard drive to be stored off site at the Society's Big Yellow Storage (currently in Luton). As an added protection when the backups prepared under clause 5 above first become obsolete they may also be sent to the Big Yellow storage.

If using web based backup facilities consider making a DVD copy of the data at six monthly intervals and sending that copy to the Big Yellow Storage as above.

- *This approach gives protection against more extensive vandalism and/or fire at the User's premises or loss at a web based facility and ensures that as a maximum only six months data can be lost.*

Note that all discs sent for off-site storage must be properly identified as to their contents and must include some adequate description to enable any third party Council member with reasonable IT skills to pick up, run and operate the files so stored.

It is another Society policy that Council members having specific responsibility for some aspect of the Society's business should have written down in a Word document full details of how their role is conducted. This file should be included in each off-site backup that is sent to the Big Yellow storage.

Some operating systems (eg MS Vista) include automated backup facilities of their own. If so then it is sensible, though only in addition to the above, to set these also to backup to the external hard drive and have the files stored in the same way. Note though that it may be sensible to use a larger sized external back up medium if these facilities are to be used and that it may not be possible (or sensibly economic) to use web based storage for such files.

Use the above approach for all your own data too – not just the Society's. The Society will store off site back ups that also include your data just as it will its own.

Finally remember that data loss is something that can happen to anyone at any time. It will happen to you at some time. Be prepared and never risk your data being lost.