# **Information security policy**

**1.** Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

**2.** In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

**3.** ‘BCY data’ means any personal data processed by or on behalf of Bury St Edmunds and District Christian Youth.

**4.** Information security is the responsibility of every Trustee, member of staff, volunteer or any other BCY associate using BCY data on but not limited to the BCY information systems. This policy is the responsibility of the BCY office and the Chair of Trustees, who will undertake supervision of the policy. Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

**5.** We will ensure information security by:

* + ensuring appropriate software security measures are implemented and kept up to date;
	+ making sure that only those who need access have that access;
	+ not storing information where it can be accidentally exposed or lost, for example, keeping hard copy data in a locked cabinet;
	+ making sure that if information has to be transported it is done so safely using password protected services or devices;
	+ taking measures to ensure the secure disposal of hard copies of personal data, for example, in the confidential waste bin on the BCY premises, after which it will be shredded.

**6.** Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If a user of BCY data has a suspicion that his/her password has been compromised s/he must change it.

**7.** Personally owned equipment which has been used to store or process BCY data must be disposed of securely. Software on personally owned devices must be kept up to date. We will not use unsecured wi-fi to process BCY data.

**8.** All breaches of this policy must be reported to the Chair of Trustees