Data Protection – Good Practice Guidelines

All organisations have a duty of care over any data they process.

BYT as a "not for profit" organisation is exempt from the Data Protection register. However, we are fully aware of the confidential nature of some of the data we hold, and as such we have created these Data Protection Guidelines, to give staff and volunteers guidance on what is good practice when handling confidential and sensitive data.

All information held by BYT is strictly for its own use. Information should not be shared with any third party without prior consent of the data subject. Everyone in the organisation has a duty to protect the privacy of information relating to individuals.

Information about individuals associated with BYT is held with the right of subject access, allowing any individual access to the information held about them.

Information held by BYT follows the basic eight principles of The Data Protection Act 1998, which are :-

- Fairly and lawfully obtained and processed
- Held only for specific purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Subject to appropriate security measures
- Only transferred to countries that have suitable data protection controls

Security Measures

- Keep files containing personal and confidential information locked away.
- Don't allow unauthorised people to be left alone with personal data.
- Do not leave any personal data in plain view in a public or easily accessible place.
- Encrypt and password-protect e-mail and database facilities.
- Keep track of any personal data that is taken away from the office through a booking in and out system.
- When deleting electronic files, ensure that they have been completely removed from your computer (i.e. empty recycle bin).
- Change passwords regularly.
- Do not pass personal data to a third party, without express permission from the subject of the information.

Protecting information from loss or damage

- Keep full backups of any electronic data.
- Protect manual files and electronic backups from fire.
- Be aware of the potential risks from computer viruses.
- Don't take documents away from the office unless it is a secure copy.
- Ensure you don't delete any files that may require keeping. If in doubt check with your line manager.