

## **Data Protection – Good Practice Guidelines**

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

Dorchester Youth Theatre as a 'not for profit' organization is exempt from the Data Protection register but as a measure of good practice have registered. We are fully aware of the confidential nature of some of the data we hold, and as such we have created a Data Protection Policy, to give staff and volunteer's guidance on what is good practice when handling confidential and sensitive data.

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

Information about individuals at Dorchester Youth Theatre is held with the right of subject access, allowing any individual access to the information held about them.

Information held by Dorchester Youth Theatre 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 rights
- Subject to appropriate security measures

### **Security Measures**

- Keep files containing personal and confidential information locked away.
- Don't allow unauthorized people to be left alone with personal data.
- Clear away any personal data before leaving the office at the end of each day.
- Encrypt and password protect email and database facilities.
- 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 expressing permission from the subject of the information.

**Protecting information from loss of 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