Securing data – 9 step plan

Introduction

As a lay officer you are responsible for ensuring data in your possession is secured. This includes data you create and process, how you store, share and transmit data and when and how to archive or delete.

Devices and services used to access and process data must also be secured, e.g., smartphones, tablets, cloud storage, third party services and online applications.

This document explains the steps and ongoing actions necessary to ensure you secure and protect members' data. It will reference individual documents on Hearth or pages in the guidance document, 'ICT guidance for lay officers'.

1. Secure all end point devices (smartphones, tablets, PCs) ensuring each has as strong a password as possible. Passwords must never be shared. (See 'strong passwords', **page 17**).

2. Protect devices by using up-to-date prevention software for AV, a firewall, encryption and anti-spyware and keep patches and updates up-to-date (e.g., Microsoft, Java). (**Pages 14-18**).

3. Secure all connectivity, e.g., networks, especially wireless networks. (**Page 10**).

4. Regularly carry out standard housekeeping. Have a schedule for backing up important data. Archive or delete data, especially if out-of-date, e.g., members' lists – case files and associated data, e.g., emails should be kept for six years. (**Pages 22-23**).

5. If storing anything important in the cloud, e.g., Dropbox, ensure data is encrypted first. http://www.teachers.org.uk/node/12170.

6. Whether you're just starting or have been an activist for years, it is good practice, wherever possible, to use the services provided by the Union. These include email, members' data and guidance. (**Page 3, page 13** and **pages 26-27**).

7. Ensure you're aware of your responsibilities towards Data Protection. (See 'Data protection: your responsibilities', **Page 24**).

   (a) Review Sharing members' data with third parties.

   (b) Follow the guidance on Hearth, 'Handling subject access request', if members make a request for their personal data.

8. On leaving your role, all data should be backed up and either handed to your successor or the Union unless you will continue to progress existing casework. Any data no longer relevant or needed should be deleted. (**Page 25**).

9. Other guidance you may find useful include:

   - Grants for ICT (**pages 13,14**).
   - Recycling old equipment (**page 25**).
   - Disability support (**pages 24/25**).
   - Social networking (**page 28**).
   - Doing surveys (**page 29**).
   - Email marketing (**pages 30/31**).