



Data Protection - Security measures

Last updated March 2026

All Elmbridge CAN staff members, as well as volunteers and trustees, need to read and apply the measures listed in this document.

1. Set up your device to lock automatically when inactive for more than 5 minutes.
2. Regularly update software and add patches without any discontinuity.
3. Make sure your personal laptop is protected by antivirus protection software.
4. Regularly review data saved on devices and delete copies when no longer needed.
5. Set up multi-factor authentication where appropriate.
6. Password protect any device and make sure you use a strong password.
7. Do not share password with anybody.
8. Do not connect to public Wi-Fi, but make use of hot spot if you find yourself in a public space.
9. Do not use your devices where your screen is visible in shared (and/or public) spaces unless you have a screen protector.
10. Avoid confidential conversations including on the telephone in public areas.
11. Avoid or password protect removable storage devices.
12. Use email encryptions (Egress) when necessary (e.g sending out safeguarding information).
13. Disable services such as Bluetooth and wireless when not required.
14. Clear desk policy to avoid leaving confidential data on your desk.
15. Locked filing cabinets, drawers or lockers for confidential paperwork.
16. When disposing confidential paper, use a shredder or disposed of as 'confidential waste'. Please contact your volunteer manager or line manager if you require a shredder to be purchased.
17. Organisational files must be saved within the organisation hosted solutions and never saved on a personal device.
18. Other members of a household that use the same device used by the ECAN staff member, cannot access any business-related information, for example, with the use of an additional account passcode (the organisation's preference is for the device not to be accessible to other individuals).
19. When a device is no longer required or is obsolete (for example because it is to be replaced) or when you leave your employment/engagement with the organisation, corporate information must be securely deleted from any personal devices.

20. Delete/upload onto Beacon or Google drive whatsapp sensitive information from your phone, and never copy/paste into AI.. More on [safe AI use and settings here.](#)