Data Protection - Security measures

Last updated September 2026 - F Buckingham

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

1. If you use a computer for ElmbridgeCAN work:
    a. Set up your device to lock automatically when inactive for more than 5 minutes.
    b. Password-protect any device and make sure you use a strong password.Do not share password with anybody.
    c. Regularly update software and add patches without any discontinuity.
    d. Make sure your personal laptop is protected by antivirus protection software.
    e. Regularly review data saved on devices and delete copies when no longer needed.
    f. Set up multi-factor authentication where appropriate.
    g. Do not connect to public Wi-Fi where possible, but make use of hot spot if you find yourself in a public space.
    h. Do not use your devices where your screen is visible in shared (and/or public) spaces unless you have a screen protector.
    i. Avoid or password protect removable storage devices.
    j. Use email encryptions (Egress) when necessary (e.g sending out safeguarding information).
    k. Organisational files must be saved within the organisation hosted solutions and only saved on a personal device for an absolute minimum time for dealing with the case
    l. 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 accessible to other individuals).

2. Avoid confidential conversations including on the telephone in public areas.

3. Clear desk policy to avoid leaving confidential data on your desk.

4. Locked filing cabinets, drawers or lockers for confidential paperwork.

5. 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.

6. When a device is no longer required or is obsolete (for example because it is to be replaced) or when you leave your employment/engagement with the organisation, corporate information must be securely deleted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.

7. Do not use your personal email address for sensitive Client information (passports, GP letters, official documents). Delete immediately after use, and in the future ask for an ElmbridgeCAN email address. You still need to delete asap, but the data will be part of our Google Workspace.

8. Delete/upload onto Beacon or Google drive whatsapp sensitive or personal information from your phone or laptop, Images of passports, visas, or official documents

9. Never copy/paste into AI anything that might identify the person, even by inference (see more, including examples in safe AI use and settings here.