Cyber Security Policy

Purpose of the policy

This policy sets out how Age UK Surrey (AUKS) will:

- protect its data systems and software from internal and external threats. For example, cyber-attacks or human error;
- ensure all information and assets are secure;
- comply with the Data Protection Act 2018 and the UK General Data Protection Regulation;
- protect personal and client data and support business continuity.

This policy should be read alongside other policies and processes on data protection, business continuity and risk assessments.

Scope of the policy

This policy applies to:

- all staff, volunteers, contractors and visitors;
- all systems, devices and information leased, stored or processed by AUKS.

Roles and responsibilities

CEO	Overall accountability and compliance
Compliance Lead	Policy oversight and compliance
IT Support (Qlic IT)	Technical security controls and support
Cyber Support Insurance	Report 0800 975 3034
Employees & Volunteers	Compliance with policy

Access to IT systems

All users must:

- have an approved user account;
- use unique log-in credentials;
- only access systems required for their role;
- have accounts removed immediately when no longer required.

Multi-factor authentication (MFA) must be used where available.

Password Security

- Use strong pass phrases or passwords?
- Do not share passwords

- Do not reuse passwords
- Report suspected compromise immediately.

Data Security and Backups

- Data is backed up regularly and securely by IT support.
- Backup access is restricted.
- Systems are tested regularly.

Cloud service providers

Our IT support Qlic IT have their Cyber Essentials and ISO 270001 accreditation, and they provide and support our cloud services.

Remote Mobile and Home Working

Employees must read also the Age UK Surrey Mobile Equipment Release Form:

- work in a secure environment;
- avoid public Wi-Fi (unless using secure approved VPN);
- lock devices when not in use;
- not allow unauthorised access;
- remain vigilant to cyber threats;
- use an authorised work device or approved personal device.

Where working away from the office employees should use a secure connection such as a work mobile hotspot.

Working from Abroad

Employees must not undertake any work activities while outside the UK.

In many countries (including the United States, India, and parts of Europe), remote working while on a tourist or short-term visa is restricted or prohibited, even for a UK employer.

Employees must not assume that short-term or informal working abroad is permitted, as visa or work authorisation is usually required.

Unauthorised access or working abroad may result in disciplinary action and removal of system access.

Access logs may be monitored to detect unauthorised access from outside the UK.

Accessing work systems when on Annual Leave

Employees are expected to fully disconnect from work systems during annual leave to support wellbeing and reduce cyber security risks.

Access to emails, systems, and files should ideally cease during this time.

In exceptional circumstances, employees may briefly carry out a check for business continuity. However:

- no operational or decision-making work should be undertaken;
- access must be via secure, approved devices and comply with all security controls;
- sensitive data must not be accessed unless authorised.

Employees should be aware that accessing systems whilst abroad may be restricted under local laws.

Use of Personal Devices (BYOD)

Personal devices must:

- be approved in advance (With Windows 11 or greater and Microsoft Defender enabled);
- be secure (password protected, updated);
- not store organisational data locally;
- not be used via public Wi-Fi unless a VPN is enabled.
- Access to AUKS apps should be through a secured OneDrive/Teams or Outlook or stored in a secure folder (APPENDIX 2)

Liability

AUKS does not accept liability for any personal devices employees bring or use when at work. Employees are responsible for keeping their personal devices safe and for insuring them.

Equipment and data security

Measures we have in place

AUKS has various protections in place to keep its digital information safe when an employee works from home or remotely.

Read these policies which relate to keeping data secure and these should be read and implemented alongside this policy:

- Mobile equipment release agreement.
- Mobile Phone Policy
- Data Security Policy
- Data Retention Procedure

Cyber Security is the set of measures taken to protect systems from threats such as hacking, phishing and malware. The following measures are in place which will help secure data used by home and remote workers include:

- staff training on cyber security.
- anti-virus software – Sophos on laptops

- rules on ensuring strong passwords given by Qlic
- secure backing up of data
- multi-factor authentication
- encryption
- email filtering
- email authentication
- mobile device management
- privileged access management (PAM managed by Qlic with authorised staff able to authorise changes to access).

Firewalls

A firewall is a type of cyber security protection which puts a barrier between a computer network and the rest of the internet. It monitors cyber traffic to and from your network while blocking anything that will potentially harm it. A firewall is only one component in AUKS's network security, and all are managed and maintained by Qlic IT.

Malware

Malware is malicious software that is put on devices which attempts to do one or more of the following:

- steal data
- damage computer systems
- cause disruption

Anti-malware software

AUKS's approved anti-malware software is Sophos.

Anti-malware software must be installed and enabled on each desktop, laptop and servers.

If employees encounter a problem with anti-malware software on their device they should contact Qlic IT for assistance.

Software and Updates

- All software must be approved, licensed, and up to date
- Automatic updates should be enabled
- Unsupported software will be removed

Third party supplier

The use of third-party software must be requested by the budget holder and approved by Qlic IT.

Third party suppliers must be able to demonstrate that they have appropriate security measures in place and evidence of up-to-date patching with regular system updates before they are approved.

A third-party risk assessment and/or vendor security assessment must be carried out. The assessment should be documented for future reference and be available for compliance purposes.

Incident Reporting

Employees must report immediately:

- phishing attempts;
- suspicious activity;
- data breaches;
- lost or stolen devices.

Devices must be disconnected from networks where necessary and reported immediately. **Qlic IT on 020 3904 3464 –to isolate your device and prevent spread.**

Do NOT forward suspect emails to Qlic or any colleagues – take a screen shot or 'snip it'.

Report the incident to your Manager and the resources team including the time and date and any actions taken.

Failure to report incidents could lead to a major data incident which could result in disciplinary action.

Compliance

Failure to comply with this policy may result in disciplinary action, including dismissal.

Review

This policy will be reviewed **annually**, or sooner following:

- a cyber incident;
- regulatory changes;
- organisational changes.

Issue	Date agreed by Age UK Surrey	Reviewed
2	Nov 2025	June 2026
3	July 2026	

APPENDIX 1

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked.**
- Keep your **devices** (and all **installed apps**) **up to date,** using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar,** or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

© Crown Copyright 2018

For more information go to www.ncsc.gov.uk @ncsc

APPENDIX 2 – Enabling Secure folder or App Lock

How to Enable App Lock on OneDrive App On APPLE device BYOD

1. **Open the OneDrive app** on your iPhone.
2. Tap your **profile icon** in the top-left corner.
3. Go to **Settings**.
4. Scroll down to **Security** and tap **Passcode**.
5. Toggle on **Require Passcode**.
6. Set a 6**-digit passcode**.
7. Optionally, enable **Touch ID** for quicker access and better security.

How to set up secure folder on Samsung device BYOD

1. **Ensure You Have a Samsung Account**
    - If not, create one here.

    1. **Enable Secure Folder**

        - Go to Settings > Security and privacy
        - Tap More security settings
        - Select Secure Folder
        - Tap Continue and accept permissions
        - Choose your preferred lock method (PIN, pattern, password, or fingerprint)

    2. **Access Secure Folder**

        - Once set up, the Secure Folder icon appears in your app drawer or home screen
        - You can also access it via the Quick Panel toggle