



**LINKS: THE CHESTERFIELD AND NORTH EAST DERBYSHIRE COUNCIL FOR
VOLUNTARY SERVICE AND ACTION LIMITED**

IT Security Policy

This policy applies to all members of staff and clients at Links CVS who use Links CVS's IT equipment, platforms and software and access Links CVS's data.

This policy clarifies for staff what they need to do to keep Links CVS's IT equipment secure and protected from viruses and malicious attacks, whether they are working at home or in the office. This policy covers: laptops, desktop computers, tablets, mobile phones and smartphones if being used for work at Links CVS.

The policy also applies to clients who use devices at the Resource Centre to ensure best practice in online safety.

Purpose

The purpose of this policy is to keep Links CVS and its staff and clients safe from malicious cyberattacks, viruses and potential data loss.

The security of equipment used online is essential to reduce the risk of problems with IT, to protect Links CVS, customer and employee confidential data (which is password protected) and business-critical information (and adhere to GDPR rules).

Over the last several years cyberattacks on businesses and charities have increased, and Links CVS must ensure it has robust systems in place to protect its data online and offline. We all have a responsibility to be alert to security risks and report anything that we are concerned about to the Chief Executive.

The policy

If you access Links CVS's data, platforms or applications on your phones and/or other devices, then you must ensure that there is adequate and up-to-date anti-virus software installed and that a passcode/password/biometric ID is required to access the device (to protect the device in the event of loss or theft).

Links CVS's anti-virus software must be installed and kept up to date on all Links CVS's devices. When new devices are set up, Links staff will ensure that this has been installed.


Links CVS's SharePoint requires a password and may prompt multi-factor authentication if you work on multiple devices.

Guidelines on how to protect your devices

It is everyone's responsibility to ensure that the IT at Links CVS is secure. Staff are required to follow these guidelines (with the help of Links CVS's ICT Support Worker if needed):

- Remove software that you do not use or need (this may require admin authorisation).
- Update your operating system and applications regularly when prompted to (this should be activated when shutting down your system).
- Store files on SharePoint so that they are backed up properly and available to all in an emergency.
- Understand the privacy and security settings on your phone and social media accounts.
- Have separate user accounts for other people if you use a shared computer.
- Require administration authorisation to install applications and software.
- Do not use an administrator account on your computer for everyday use.
- Ensure that your devices log out automatically after being inactive for 15 minutes and require a password/passcode to log back in.
- All staff will receive training about IT security. We use Get Safe Online (www.getsafeonline.org) which is a good source for general awareness.
- Use extreme caution when opening email attachments (especially unexpected attachments from any sender) or clicking on links from unknown senders or on social media.
- Be wary of fake websites or social media platforms.
- Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website and that such disclosure is in line with Links CVS's Data Protection Policy.
- Use social media, including personal blogs, in a professional and responsible way, without violating Links CVS's policies or disclosing confidential information.
- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- If any of your devices get lost or stolen, report the incident to your line manager as soon as possible.

This policy is not a definitive statement. You should at all times be mindful of IT security and take steps to ensure that you are not doing anything that could harm Links CVS or its staff & clients.

Approved by Links Board:	
Date:	10 th June 2025
Signature:	
Review Date:	10 th June 2028