

IT Security Policy

Who is covered by this policy?

All members of staff, trustees and volunteers at Suffolk Artlink who use Suffolk Artlink's IT equipment, platforms and software and access Suffolk Artlink's data.

What is covered by this policy?

This policy clarifies for staff and volunteers what they need to do to keep Suffolk Artlink'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 Suffolk Artlink.

Purpose

The purpose of this policy is to keep Suffolk Artlink and its staff, volunteers, trustees and customers 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 Suffolk Artlink, customer and employee confidential data and business-critical information (and adhere to GDPR rules).

Cyberattacks on businesses and charities have increased, and Suffolk Artlink 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 General Manager.

The policy

If you access Suffolk Artlink'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 or password is required to access the device (to protect the device in the event of loss or theft).

Suffolk Artlink's anti-virus software Bitdefender must be installed and kept up to date on all Suffolk Artlink's devices. When new devices are set up, ensure that this has been installed by the General Manager. If in doubt about whether it is installed on your Suffolk Artlink's device, raise it with the General Manager.

Suffolk Artlink's cloud-based office software, Google Workspace and Office 365 Business Basic, requires a password and two-factor authentication.

Suffolk Artlink recommends that you switch off all Suffolk Artlink's devices at the end of the working day to help ensure that the anti-virus software is regularly updated as required.

With electronic equipment, you should not use the device to store Suffolk Artlink's work on the desktop – it must be saved on Suffolk Artlink's cloud-based storage.

Guidelines on how to protect your devices

It is everyone's responsibility to ensure that the IT at Suffolk Artlink is secure. Staff are required to follow these guidelines (with the help of the General Manager and support provider Atec Solutions 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 [cloud-based storage] 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.
- Take time to learn about IT security and keep yourself informed. Get Safe Online (www.getsafeonline.org) is a good source for general awareness and is an induction requirement.
- Use extreme caution when opening email attachments (especially unexpected attachments from any sender) or clicking on links from unknown senders or on social media. (Staff may view header info / show original to check sender details and for DKIM and DMARC pass.)
- 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 Suffolk Artlink's Data Protection Policy.
- Use social media, including personal blogs, in a professional and responsible way, without violating Suffolk Artlink'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 Suffolk Artlink or its staff.

See also Data Protection Policy and Cyber Safety Policy.

Monitoring and Review

The Board of Trustees will review this policy triennially.

Date	Signed	Role
20/07/2026	Alistair Winch	Company Secretary on behalf of the Board of Trustees