Argyll and Bute Third Sector Interface
Cyber Security – working safely and securely

Working remotely can mean that it is harder to secure your data against cyber-attack. It can seem hard to find the balance between supporting easy access to systems and managing them securely. It is essential you have good cyber awareness and contingency planning in place.

Three key actions

- **Have a cyber-security policy**
- **Instigate an organisational culture of working safely**
- **Train your staff on online safety and privacy**

Cyber security policy
Your board/trustees should work with senior management to identify risks and protection measures to put in place. A written policy should be produced with information on what to do in the event of a cyber-attack; who needs to be informed; and which gives clear guidance to staff on their day-to-day responsibilities.

You may also decide to get your organisation Certified in Cyber Essentials, a government- backed scheme.

Organisational culture of safe working
You should encourage your people to be curious and report any issues to senior management. If you regularly pressure your staff to just get on with things, then you risk them losing their natural curiosity to evaluate things and spend time flagging up anything concerning
You should also keep yourself up-to-date on security issues and shut down scaremongering conversations, which are often fueled by tabloid headlines and social media.

It can be difficult for people to know what to believe, so you should promote the truth and validity of just a few trusted sources to prevent the overwhelming amount of information available. Our trusted sources are NCSC (National Cyber Security Centre), Scottish Government's Cyber Resilience Unit and Get Safe Online.

You should also provide and manage devices which will make it much easier to ensure key security settings are applied and kept up to date.

Train staff on online safety and privacy
You should provide staff with regular training on online safety and cyber security. Any reported incidents should be circulated to all staff to remind them to be vigilant and to encourage reporting.

You should regularly remind staff to of safe working practices, such as:

- Only connect to secure WiFi networks – change the default password on your home WiFi router.
- If you are away from home, never use public wifi – using your mobile phone as a hotspot is safer
- Ensure your computer software is up-to-date and that antivirus and malware scans are run regularly
- Use a password manager, like LastPass, to ensure passwords are strong and unique and not written down anywhere. If you share a device, ensure that you use a separate, password-protected user account for any work-related activity.

Argyll and Bute Third Sector Interface
Cyber Security – working safely and securely

- Ensure that you back up files you have been working on. This is automatic if you work in the cloud.
- Consider using a privacy screen for your laptop, and screen, so other members of their household cannot see the screen
- Always lock your device if you're having a break – the keyboard shortcut to this is Windows-L.
- Make phone or video calls from a private room, if possible, and if this is not possible a headset will keep callers' information private.
- Be mindful of what you let people see in the background on video calls, e.g. confidential paperwork or a way to identify where you live.
- Stay curious and vigilant – verify any unusual requests you receive from colleagues, like payment requests, changes of bank details or password resets – these may be phishing attacks or scams.
- Work in the cloud as much as you can to minimise the amount of information you have to store on a local computer
- Regularly clearing browser history and the Downloads folder
- Enabling multi-factor authentication
- Enabling encryption on the computer hard drive

Argyll and Bute Third Sector Interface
Cyber Security – working safely and securely

Published on the Argyll and Bute Third Sector Interface Self-Serve system (www.argylltsi.org)
(Adapted from SCVO)

Version: 1.0
Published: June 2020
Review date: June 2021