

# HOW TO START A WORKPLACE CONVERSATION

## CYBER HEALTH AND SAFETY

The cyber security of your workplace is not solely a technical issue. All employees, from the owner or manager to the front desk, have a role to play. Cyber security is about protecting the information that belongs to your workplace – whether it is your organisation’s intellectual property, financial information, details of your customers or personal staff details.

Employees are the company’s greatest asset – but also potentially the biggest risk. They are the best line of defence, but also a vulnerability. Even the best security can’t protect you if you leave your information “unlocked”.

## WORKPLACE POLICIES

- **Acceptable Internet use:** Include a workplace policy about acceptable Internet use in your employment agreements.
- **Email address:** Have a workplace policy about appropriate use of work email addresses for signing up to email lists, newsletters and websites (e.g. online shopping, mailing lists). You should not send sensitive work information to your personal email addresses.
- **Installing programmes:** Have a workplace policy about using or installing new programmes or applications (e.g. games) on the work computer, laptop or work mobile devices. Installing unapproved programmes can expose the work network to vulnerabilities.
- **External devices:** Have a workplace policy for using devices such as USB sticks, DVDs, MP3 players and smart phones at work. Plugging them into the work computer could expose the work network to a virus or malware. Either do not use them on the work system or ensure they are security scanned first.
- **Updates:** If appropriate, ensure that employees keep their operating systems, security software and apps up to date on their computers and mobile devices.
- **Back-ups:** Have a workplace policy and systems in place to regularly back-up important data and test that it works.

## PASSWORDS

- Make sure all critical accounts have strong passwords. Connect Smart recommends using a combination of lower case and upper case letters, numbers and special characters.
- Have different passwords for different accounts, and consider using password managers.
- Consider using two-factor authentication if it is offered by the service for an added layer of security.
- Do not write down your password and never leave it in an obvious place e.g. on a sticky note or a file marked “passwords” on your computer. Don’t share them with anyone else!
- If your workplace does not have an automatic prompt to change your password every four weeks, then set up a calendar reminder to do so.

## WORK LAPTOPS AND WIFI

- Secure your workplace wifi with a password. Change the network name (SSID) from the default – this will make it more difficult to find out what the router make/model is and harder for unauthorised users to gain access.
- Make sure that the encryption feature is activated on your laptop – this is an important control to protect data and all modern operating systems offer this feature built in.
- Don’t use public wifi for anything that needs a login.
- Ensure everyone has their own password when using a shared network or computer.
- Lock the computer – when employees leave their desks, they should lock their screens or log out to prevent any unauthorized access. Laptops must also be locked when not in use.
- Do not leave your work (or personal) mobile device lying around where it can be stolen or tampered with.

