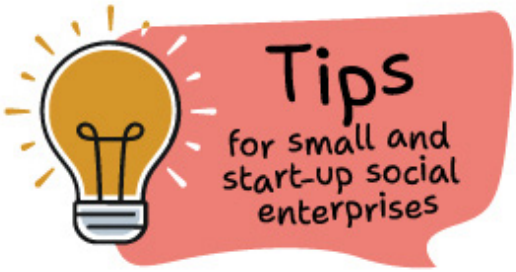
Managing data *safely and securely*



Keeping data safe and secure is a worry for many small businesses, including social enterprises. Here are some tips shared in the data learning community for managing data.

We have also included links to useful resources on cyber security.

Cyber security is more about people than technology

Cyber security sounds like something that requires a lot of technical expertise, so people are often surprised to learn that most cyber incidents in small business involve human error.

Examples or errors might include:

- paying a fraudulent invoice
- giving the wrong person access to banking information
- clicking on a scam link.

This means that staff training and awareness can make a huge difference to your data security (see links to free resources in the box to the left). It's also worth thinking about how data issues are covered in your policies and procedures, such as having an AI policy, privacy policy and confidentiality policy.

Build a culture where people are willing to share mistakes

Even the most tech-savvy person can fall for a scam, especially if they're busy and distracted. It's also getting harder to spot scams with increasing use of 'deepfakes' (editing images, video and audio using AI). If people hesitate to report a mistake because they're embarrassed or worried about getting into trouble, it can delay an effective response. Build a culture in your team where people are willing to share 'close calls' and feel able to let you know if something has gone wrong so you can address it quickly.

Make the most of free resources and training!

The Cyber Wardens program provides free training and resources to help protect small businesses from cyber threats. They have foundational topics, such as learning to recognise the 'red flags' for scams, and the bad habits that reduce online safely. They also have more advanced topics, such as AI safety and creating an Incident Response Plan.

cyberwardens.com.au/campaign/the-data-conversation/?source___course_enrolment_level_1=the_data_conversation

You can also check out the resources at the small business hub at the Australian Cyber Security Centre, including guides for securing Apple, Google and Microsoft systems, and a free cyber health check tool to help you do a basic cyber security assessment for your social enterprise.

cyber.gov.au/business-government/small-business-cyber-security/small-business-hub

Give people the right level of access

When it comes to data access, think of Goldilocks: not too much and not too little. 'Just right' looks like people having access to all the data they need to do their job, but nothing more. The more people who have access to data, the higher security and privacy risks.

As an example of good practice, a social enterprise that has volunteer staff might give everyone in the team access to the list of volunteers and their availability, but only the volunteer manager would have access to working with children checks or address details. A case management or client management software system should have options for tailoring user access to data. If you don't have this kind of system yet, even simple steps like having separate spreadsheets or separate folder access will help establish appropriate access levels.

Continued over the page

If something goes wrong, help is available

IDCARE is Australia's national identity and cyber incident community support service. Their Small Business Cyber Resilience Service offers free expert support to help Australian small businesses and sole traders recover from cyber incidents.

idcare.org/ 1800 595 160

The Australian Cyber Security Hub has guidance on how to report and recover from cyber incidents, including data breaches, compromised business emails, identity theft and hacking.

cyber.gov.au/report-and-recover

Keep your systems up to date

Software and app updates can be annoying but these updates are often required to fix security vulnerabilities. It's a good habit to fully shut down your computer at the end of the day. You can make this less onerous by pinning or favouriting documents that you use regularly, and by using tab groups or bookmarks to store the webpages you're using.

Another tip is to take stock of all the software and online platforms you use in your social enterprise, so you have an up-to-date list. Then you can work through to this list to review the security features and check you have appropriate options enabled, like enabling multifactor authentication (MFA). MFA means you need a combination of different types of authentication (including passwords, secret questions, phone, or facial recognition) to access an account, improving account security.

Your software list will also be useful if someone leaves your organisation, so you can systematically check you've removed their access.

Manage your passwords

A good password manager is one of the most important tools for your social enterprise. It can help you generate unique and strong passwords, store them safely and alert you if any of your passwords have been exposed in a data breach. Even if you're a small social enterprise, it can be worth investing in a business password manager, to help you share details safely across the team.

Lock your screen!

If you're going to be away from your computer, don't forget to lock the screen. If you learn the keyboard shortcut, it will only take a second (on Windows it's **Windows key + L**, while on a Mac it's usually **Control + Command + Q**). This is particularly important if your screen can be seen by people walking past your desk, or if you work in a public space, like a coffee shop.

THE DATA CONVERSATION
Spreading the power of data, one conversation at a time

The tips on this sheet come from the data learning community for small and start-up social enterprises. The data learning community was hosted by The Data Conversation and commissioned by Social Enterprise Australia as part of the Australian Government's Social Enterprise Development Initiative (SEDI).

w: thedataconversation.au **e:** enquiries@thedataconversation.au