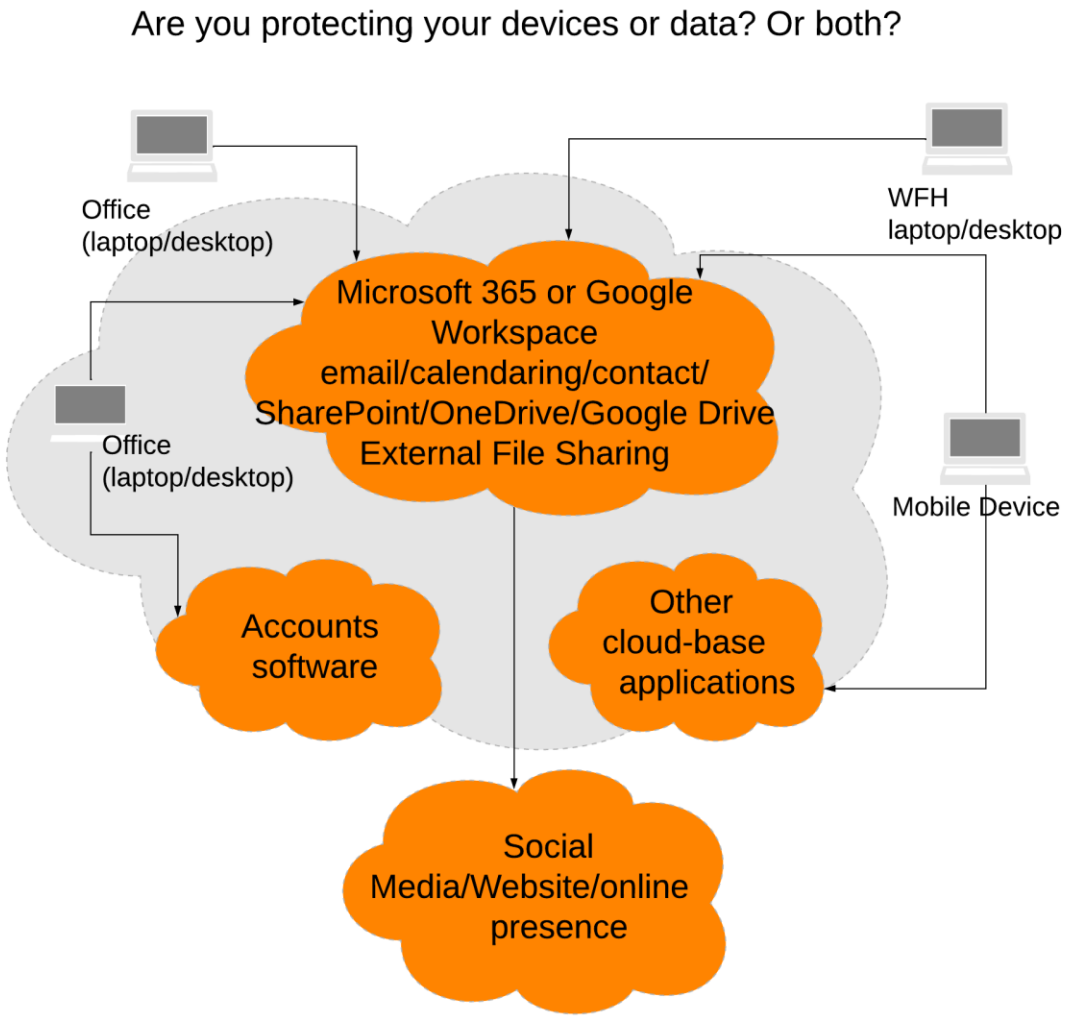
7 WRITTEN IT POLICIES ALL ORGANISATIONS SHOULD HAVE

Make it easy to stay safe

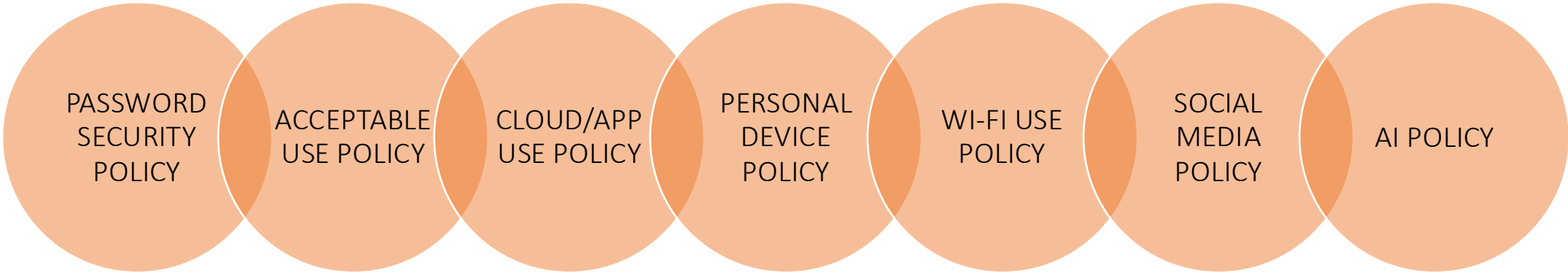
How do IT policies protect my business?
Cloud-based data that is accessed on multiple devices needs protection: a breach on one laptop could spread to the whole organisation.
Policies define how the devices and data are defended



Introduction

- Why does my business need IT policies?
- Your team are the front-line of your cyber defence. They are your human firewall.
- Varying IT knowledge. Don’t assume people are tech savvy.
- Make it easy for your team to know what safe looks like.
- IT policies take the guesswork out of how to transact online.
- Increased risk when they are no policies.
- Increased confidence when these policies are written and enforced.
- Write them once. Broadcast regularly. Review annually.

WHAT ARE THE POLICIES?



PASSWORD SECURITY POLICY.

- Passwords are one of the weakest links in IT security because humans are not great at remembering unique, complex and random passwords.
- Use upper case, lower case, numbers and symbols.
- Any three words. Non-dictionary words.
- Password managers are your friend.

ACCEPTABLE USE POLICY.

- Charter of how your team use IT in the organisation
- Removes uncertainty. Provides clarity.
- Separation of work from personal. Don’t save work data to personal storage.
- Enhances data security. Ensures compliance.
- Minimise risk.

CLOUD AND APP USE POLICY.

- Define what is work data.
- Explain the risk of data leakage.
- Discuss what data is confidential and what is public
- Provide guidance on what safe cloud working looks like.
- Minimise risk.

PERSONAL DEVICE POLICY

- Personal devices belong to the person, not the org. How much control can you have over it?
- Is the device secured with approved work security software and controls?
- Who can install apps on it?
- Minimise the risk of cyber attack on the device.
- Minimise the risk of data loss/leakage/theft

WIFI USE POLICY

- The dangers of public WIFI
- “Free” WIFI is not secure
- Who is “listening” on the free WIFI network?
- How dodgy WIFI networks can steal usernames and passwords.
- What is a VPN and how can it help to keep you safe?
- Minimise risk.

SOCIAL MEDIA USE POLICY

- Social media is the public profile of your non-profit
- Protect reputation
- Personal views Vs Organisational views
- Hours of posting.
- Make sure you protect access! MFA, MFA, MFA!

AI POLICY

- Ensure all AI tools used have a data processing agreement in place with your business.
- Train your team on security, where not to add sensitive/personal data
- Check legal contracts with clients and suppliers
- Setup approval process for new tools.

When are these policies shared with your team?

Once written share with everyone in a meeting and talk it through.

When a new starter arrives. Don't assume they will get it by osmosis!

Regular reminders (at least annually)

Ensure all policies are accessible in your work data area (SharePoint or Google Drive, etc)

Those orgs considering Cyber Essentials will have to have some of these anyway.