* 1. **I can take appropriate steps to avoid risks when working with collaborative technologies including complying with guidelines**

Keeping personal information limited online, for example names and addresses and email details should not be shared out (unless it’s sent to a trusted person/website), sending bank details to people via apps (unless secure). Email address used shouldn’t contain names and other personal details. VPN (virtual private network) creates a secure connection when surfing the internet, it provides an extra layer of privacy and anonymity, but it costs. Keeping privacy settings on can keep marketing companies from taking personal data. Practicing safe browsing, avoid browsing dangerous/risky websites, can save you from becoming a victim of identity theft and your device getting malware. Saving passwords on your device is not wise as some hackers can get access to it, so it’s best to either memorise or keep it in a safe location, like a trusted password manager software. It’s also a good idea to choose strong passwords rather than weak ones. When going online in a public area, making sure your internet connection is secure is a must, especially if you’re going to be dealing with personal details, bank details and sensitive information. Keeping antivirus software up-to date is vital, as it provides your device with security against malware.

Online use policy, an example of violation to the policy, could be using social network sites, a fake email, tools, or messaging services to intimidate and harass another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail/messages, or by using someone else's name or User ID.

Copyright protects peoples work and stops others from using it without their permission. Copyright protection is automatic, when original content is created, to use that content, the owner’s permission would be needed. If content that has copyright is used without taking consent of the owner, you could be faced with fines, and depending on the severity even imprisonment.

* 1. **I can explain what risks there may be in using collaborative technologies and how to keep them to a minimum**

Some risks of using collaborative technologies:

Unfortunately, Identity theft is a very common issue online, to prevent it, personal information should not be disclosed online, unless you are fully aware and trust the site you are disclosing your information to educate yourself more into online security, and how to prevent becoming a victim, also having a security software installed on devices can prevent from many online security issues/viruses, avoid questionable websites, only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them.

Cyber bulling is any form of bullying which takes place online, the impact can be very damaging to the victim, so prevention should be priority. Cyber bullying can be through social media, emails, messaging apps. It can be in many forms, one of which is harassment-this is the act of sending insulting, abusive, threatening, rude, humiliating, offensive messages. It can be offensive comments on posts, photos, videos on social media sites, chat rooms, emails and gaming sites. Ways to prevent and stay safe from cyber bullying, is to create strong passwords, use privacy settings where available, keep accounts private.

Misuse of images online is common, unfortunately once its online, there will be many risks around it, so you should be very mindful of what is posted online. Images can be copied and used to impersonate that individual, it can be put on websites to create fake profiles, sometimes to tarnish individuals’ reputation, and create false identity. Adding copyright or a watermark will help prevent to a certain extent, but not completely.