Jesus College Oxford

Seven IT things which commonly trip up students

1) **Make sure everything you create is properly backed up.** Your laptop can break, get stolen, dropped or lost and if you haven't got a current backup then you are going to be in a very bad situation. Your SSO account comes with 1TB of OneDrive space – Microsoft's Cloud drive. Use this, or Google Drive, Dropbox or whichever you prefer, and keep all your work there. If you use Microsoft's OneDrive app then it will appear just like a normal drive on your laptop, making it very easy to use. If you can, do a whole-disk backup as well from time to time – this will be very useful if you should ever need to do put the whole laptop back to its previous state.

2) **Test your OneDrive or whatever to make sure you can retrieve files without your laptop** – log in from another PC and check that what you think is in the Cloud is actually there. OneDrive also does versioning, meaning that you can easily go back to earlier versions of a file. Have a play with this and make sure you understand how it works and how to roll back.

3) **Be careful carrying bottles of water around in your rucksack or holdall along with your laptop.** If the bottle leaks or bursts, that can be the end of your laptop.

4) **Make sure you're running a good anti-virus and anti-malware software.** Sophos is available free of charge through the University's IT Services website – http://it.ox.ac.uk

5) **Forgotten passwords are the most common cause of login problems.** Use a good Password Manager/Vault so that you don't fall foul of this Keepass is a good vault product – one master password keeps all your other passwords safe, but easily retrievable when needed. But make sure you don't lose the master password or you will have lost everything inside the vault.

6) **Be very careful what you click on** – there are a lot of scam emails around which will try to get you to log into bogus websites in the hope of capturing your login details (often called phishing), others will try to get you to install ransomware on your laptop or take you to websites which are infected with malware. It can take a lot of time to recover from this kind of attack so may sure you only click on links once you've satisfied yourself that it's genuine, no matter who has apparently sent you the link.

7) Use multiple methods of MFA (multi-factor authentication). MFA is required for SSO logins – but don't configure just one method. We recommend the Microsoft Authenticator plus one other method – the snag with Authenticator is that it's tied to your phone's hardware. If you lose or break your phone, you cannot just install Authenticator on another one and carry on – it won't work. Instead, when you set up Authenticator, configure another method as well – phone call or text message for example.