**3.1.** **1 I can take appropriate steps to avoid risks when working with collaborative technologies including complying with guidelines**

When using social media I am mindful of my privacy online. I ensure that my privacy settings are set to the highest level of privacy; giving only people I am friends with permissions to view my profile. I do not post personal information online such as my address, date of birth and telephone number. I do not add people I don’t know to my social media profiles. I do not post pictures online to avoid the potential for people to use my pictures to set up fake accounts.

When using social media platforms I abide by their acceptable use policies by not ‘trolling’ other users, using a fake profile or posting material that is abusive or offensive.

I use different passwords for my online accounts rather than using the same password for every site. If the security of one website is compromised your information could be leaked and your email and password could be entered into other websites to try and gain access. I use capital letters and numbers to ensure my password is strong and I do not use obvious phrases such as ‘password’ or sequential numbers like ‘12345’. I try not write my passwords down unless absolutely necessary and if I do I only wrote down part of the password to remind myself, I would never write down all of my passwords in one place and in full in case they were accessed by someone else.

In my job role I work with patient and staff data on a daily basis. It is not permissible to transfer information from one database to another and data must only be used for the purpose it was collected for. For example we are not allowed to send patient information via our normal email but must use nhs.net which is an encrypted email service provider. I must adhere to the data protection act, Caldecott principles and the contractual guidelines of my workplace to ensure data is only used with consent, is accurate and that it is kept secure