3.1 I can describe what access rights and issues other people may have in using collaborative technologies

When using collaborative technologies, users will have been given different levels of access privileges dependent on their reason for needing to access the applications or data. The security of information and systems are an important factor when deciding on the level of permissions to give a system user. For example, as part of my job role I have full access to personnel files including permissions to read/write, delete and modify files. To have these access permissions they had to be requested and justified by my line manager and then further authorised by the IT department. If someone who did not have these permissions tried to access the Personnel Files they would receive an error message ‘Access denied, contact systems administrator’. This means that only the relevant personnel who need access as part of their job role can access the files.

All changes to network permissions within my organisation must be requested via our IT department with additional authorisation from a line manager (who must give justification for requiring a new/ altered permission). I work in a health care setting which uses multiple systems to access highly confidential patient information which is subject to data protection laws. If everyone was to have open access to this data then patient confidentiality would be severely compromised therefore breaking the law and severely impact the organisations reputation. The date could be accessed by everyone, for any purpose, including illegal purposes and important data could also be lost.

For this reason every single system used within my organisation needs access permissions that include a password requirement. Only a very select number of people within my organisation are able to make changes to the IT systems and there are very stringent security protocols in place to prevent damage and exploitation of the organisations network.

There are two main differences between the authorisation and authentication process at my workplace. When accessing the personnel files at work I do not need to enter a password as I have already been **authorised** to access them. However when trying to access a system such a logging on to the network or to use an application to retrieve patient data I need to use a password as part of an **authentication** process to verify who I am. Other steps within the authentication process can also include passcodes, handprints and security questions.