**3.1 I can describe what access rights and issues others may have in using collaborative technologies**

Depending on what a user needs to perform their job tasks, the rights they may be allocated may be minimal or complete.

Someone in an IT support role/ webmaster will need the ability to create and erase data, as well as everything in between. Without these access rights, they would encounter issues when trying to make changes to the collaborative technology they are charged with.

Conversely, someone in a relatively junior or admin-based/ data entry role may only need the ability to create and read data. If given more substantial access rights someone could cause immeasurable damage to an organisation. Such damage may include to information, if files are mistakenly deleted or viruses/ malware is downloaded. Alternatively, someone may share data with a third party causing damage to a the reputation of the business and potential fines.

Additionally, if someone has the authorisation to do something but they are not able to pass authentication checks then they will have an issue performing efficiently.

In summary, if someone does not have the access rights that they need to perform a job function then they are going to have problems in working effectively. Thus, someone in a senior role may need numerous access rights to do their job, whereas someone doing junior/ data entry will not and may cause issues if they do. Generally speaking most people will be given the most basic rights, and then given more if they are needed. Policies and procedures are put in place for people that aren’t able to pass authentication checks, such as forgotten password/ username routes.