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

Reasons why different rights are needed for different users in a collaborative community, is because not everyone will have the equal rights and authority to access certain types of data/ information in that company, depending on their position. Access rights are the permissions an individual user or a computer application holds to read, write, modify, delete or otherwise access a computer file; change configurations or settings, or add/remove applications. An organization’s network or information technology administrator can define permissions for files, servers, folders or specific applications on the computer. If access rights were given to everyone equally, it could prove disastrous, inexperienced users could end up accidentally deleting, damaging, or even stealing valuable and sensitive information which is confidential, information which otherwise should only be accessed by senior authorised users, this is where security comes into place, like having passwords for basic level users, with limited access to information. Higher level managers and officers have access to evaluate and, if necessary, revise business models or strategies and make other decisions that affect the organization. In a secure environment, authorisation follows authentication.

Authorisation gives users permission or denies the access to resources. Authorisation can give the user access to specific resources, or all resources, depending on who the user is.

Authentication is a security process, to confirm/verify, that the user is who they claim to be. Authentication can be passwords and usernames – this is the most common one, one-time pins, to get one off access, biometrics- fingerprint or eye scan, and in some instances, there may be more than one security factor to grant access known as multi-factor authentication, this would be in place to increase security beyond what passwords alone would provide.