**M3 - ethical decision making in organisational IT security**

Ethics is important to consider in IT security, as privacy, rights, and security are all related, overlapping fields.  
For example, is it OK to monitor every website an employee visits in order to check if they break the IT policy? Similarly, is it OK to allow the employee complete privacy, but not know if they have broken the policy? Both arguments have their merits, so it is important to consider ethics when making an IT policy in order to get the best of both scenario’s.

**Freedom vs Security**  
In a perfect world, users could do anything they wanted and systems would remain secure. In practice, this is not possible, so IT policies limit user’s activities to keep the IT system safe.  
Many aspects of policies seem clear-cut. For example, users should only have access to their own account, and not share it or attempt to use others. Problems come in when there is a security breach because somebody broke the policy. Is it then acceptable for an administrator to access the user account?  
Some organisations will decide on a case-by-case basis, others may plan ahead and answer the question in advance. It is good practice to make sure this is covered in the policy, both for the ethical reason of informing those who agree to the policy, and for legal reasons, such as an employee suing the organisation for breach of privacy or violation of the contract.

**Privacy vs Security**  
It is not just users within the organisation that need to be accounted for. The Data Protection Act prevents organisations from sharing client data without consent, but does not prevent them from viewing the user data. In the case of a file storage service, the data may be extremely personal, such as photos or a journal.  
However, the file storage service is not allowed to host illegal content such as copyrighted material or information that is illegal to possess (for example, classified government intelligence that has been leaked or stolen). The organisation has to protect the user’s privacy and check that they are not uploading illegal content. Some file storage services deal with this by asking the user to agree to terms and conditions stating that are liable for illegal content, or that the organisation may check to see if uploaded content is illegal. Other, more privacy-oriented services, may encrypt all user data, meaning that nobody but the user can access it, and therefore the organisation is cleared of responsibility.  
It is because of situations like this that many politicians want ‘back doors’ built into encryption systems, and to increase public surveillance. While this may increase security, whether the security-to-privacy ratio is ethical is still up for debate.