Acceptable Use Policy

**Responsibilities of Users:**

Ensure the device that they are working on is secure.

Work in a private environment.

Keep learning resources private unless you are authorised to redistribute them.

Work only with devices that you are authorised to use.

Being familiar with the computer Misuse Act 1990 and what constitutes to an offence.

**Unacceptable Uses:**

Using the knowledge learned in the classroom to gain unauthorised access to a system

Tampering with data on a system that you are not authorised to use.

Using knowledge learned in class to supply or create malicious programs.

Sharing private and/or secret data that one has access to.

Using knowledge learned in class to create and/or distribute programs or software that can cause damage, gain unauthorised access to or change a system unless done for educational purposes.

Acting with intent to cause damage to a system that you are not authorised to use.

Collaborating with intent to damage a system in a Distributed Denial of Service attack.

**Potential Consequences to My Career:**

Not being able to find a computing job or a job in the public sector, or any job that handles private and/or secret data.

Potentially having a bad reputation as a malicious hacker.

Monetary cost with a potential decrease in wages throughout your whole working life.

Being prohibited or limited on using a computing device.