Student Guide:
I.T. Acceptable Use Policy

I.T. Acceptable Use Policy

What is the purpose of the policy?
This policy has been created to define the term of acceptable use of information technology throughout the College.

Who does it apply to?
All staff, students, visitors, volunteers, contractors and Board members.

What does it cover?
It covers:
- Computer hardware.
- Computer software.
- Network services.
- Databases.
- Digital signage.
- Storage devices.
- Email.
- Telephones.
- Instant messaging.
- Printers.
- Wi-fi.
- All College systems e.g. intranet, My City, etc.

What do I need to know?

- It applies when using College I.T. resources both on-campus and off-campus.
- You will have access to the College I.T. resources from the start to the end of your course.
- College I.T. should be used to support your learning.
- Users must not use the College I.T. systems to access, send or store unacceptable content. This includes content (but is not limited to) that is:
  - Illegal.
  - Likely to promote illegal acts, goods or services.
  - Likely to promote terrorism or violence.
  - Obscene, indecent or pornographic.
  - Commercially restricted or in violation of copyright.
  - Like to cause business or reputational damage.
  - Defamatory, malicious or abusive.

- o Offensive,
- o Likely to bully, harass, victimise or discriminate against another person or group.
- You must only use your own log-in.
- Do not share your log-in details with anyone else.
- Misusing the College I.T. resources includes (but isn't limited to):
  - o Vandalism or deliberate physical damage to I.T. equipment.
  - o Unauthorised access to any system or other user's account.
  - o Impersonating another user (e.g. sending messages that appear to originate from another person).
  - o Sending chain or unauthorised bulk messages (SPAM).
  - o Misrepresenting the College using a College email account or College branding.
  - o Activities for commercial gain (e.g. running a business, non-College advertising etc.).
  - o Personal use which incurs a cost to the College (e.g. premium rate telephone calls, bulk printing etc.).
  - o Using unauthorised or unlicenced software.
  - o Introducing viruses or other malware.
  - o Causing denial of service or impacting system availability by congesting or disrupting College systems.
  - o Breaching or attempting to breach security controls.
- I.T. systems are set up to filter and block some content, although this can't always be guaranteed. You must ensure you act responsibility when using the College I.T. systems.
- The College provides students with their own data storage drive. Critical work should be backed-up to your own personal device/cloud based storage. We do not retain the content of these drives at the end of your course.
- The College monitors user activity.
- Student email accounts are provided by Microsoft and as such are monitored as per Microsoft's own terms and conditions.
- You are responsible to ensure your abide by the Policy:
  - o For less serious breaches, users will be given advice on ensuring adherence.
  - o For more serious or repeated breaches the College's Disciplinary Policy and Procedures may be triggered.
  - o If an offence has been committed, the College has the right to contact the appropriate authorities.

You can view the full policy here.