Online Safety Policy

Last reviewed: Tuesday, September 10, 2024

Melton College runs courses for families, older adult students (aged 40+) and for juniors. We manage our own Homestay provision, and also run a small hotel in the building next to the College. Our Policy documents relating to Safeguarding are review at least annually, with the review date shown under the title. It circumstances dictate, the policies are review more regularly, for example in response to an incident or to take account of statute.

Melton College, York recognises that it has a duty of care to ensure that all students and staff are able to use the internet and related communications technologies appropriately and safely.

Students and staff are made aware of online safety issues, what constitutes inappropriate and/or unacceptable use.

We recognise that the best way to prevent, or at least minimise, inappropriate or unacceptable use is through online safety education.

Staff have online access via the College network, using either college devices or their own devices. Students have no access using College devices. They have access using their own devices via the College Wi-Fi but it is important to acknowledge that an increasing number of students access the internet via their own device and using their own data allowance. This reality makes education all the more important as we have, in effect, few if any physical restraints to access.

Online Safety Issues Include But Are Not Limited To:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- Examples of unacceptable use of the internet/communication technologies by students and staff:
  o viewing/sharing/sending offensive, sexually explicit or harassing material or any material which promotes radicalisation or extremism
  o Publishing defamatory and/or knowingly false material about Melton College, York or any of its course participants
  o Engaging in any kind of illegal online activity including infringing copyright or gambling

The Designated Safeguarding lead (DSL) will take the lead in promoting online safety and appropriate use

Staff Responsibilities:

- The first responsibility of staff is to understand that online safety is a part of safeguarding. They will report any suspected misue or issue, they will monitor any use of digital devices in lessons and other activities and that all infractions will be reported
- Follow the Staff Code of Conduct (Available in the info centre on the website, in the staff area on the website and made available to Group Organisers and Leaders) regarding social media and the sharing of email/phone numbers
- Embed online safety education into classes, activities and student meetings as appropriate for the students' age and level of English.
- In lessons/activities where internet use is pre-planned, students are guided to sites checked as

suitable for their use.
- Staff should be guided by an awareness of the 4 Cs
  - Content
    - Movies/clips shown to students during class or social activities must be appropriate for their age e.g. no 15-rated films for under 15 year olds.
    - Internet videos e.g. YouTube clips used in a class or activity must be checked all the way through in advance to ensure the content is suitable.
      - *Staff should also be aware that their previous search history, which may be inappropriate, may show up when they are sharing their screen*
    - Ensure any songs used in class/activities are the 'radio edits' which do not contain inappropriate language

  - Contact
    - Be alert to and aware of student behaviour when students are accessing personal IT devices (phones, tablets etc.) and monitor if necessary. Student behaviour can indicate inappropriate contacts or groups
  - Conduct
    - Be alert to and aware of student behaviour when students are accessing personal IT devices (phones, tablets etc.) and monitor if necessary. Student behaviour can indicate inappropriate uses of IT and/or online bullying.
  - Commerce
    - Be aware of the use of monetized sites and gambling sites

Student Responsibilities:
- Understand the need to report abuse, misuse or access to inappropriate materials and know how to do so
- Be aware of the need to use social media with care and withing the community guidelines of the provider
- Understand the rules relating to the taking and sharing of photos/videos and online bullying (see Anti Bullying Policy)
- Understand the importance of online safety

Responding to Incidents of Misuse:
If a student or staff member is discovered accessing inappropriate or illegal material, staff are required to ensure the student/staff member stops viewing it immediately and take the following steps:
- Report the incident to the DSL using either the Low Level or Major Safeguarding Concerns Form
- The DSL will speak to the student/staff member and ensure he/she understands why the material is inappropriate and that it should not be accessed again
- If the material is suspected of being illegal, the DSL will take appropriate action which may include contacting the Police and/or starting disciplinary procedures