Student Social Media & Online Safety Guidelines

1. Definition of social media

1.1 For the purpose of these guidelines; social media is defined as a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Discord, Threads, Snapchat, Facebook, and LinkedIn. Social media also covers blogs, podcasts and video and media sharing websites such as Instagram, YouTube, and Flickr.

1.2 Appendix 1 – provides further examples of social media platforms, however students should be aware that there are many more examples of social media than can be listed here and this is a constantly changing arena. Students should follow these guidelines in relation to any social media that they use.

2. Purpose

2.1 The purpose of these guidelines is to support students to develop an online social media presence that is ethical and legal while taking full advantage of the benefits of using social media technologies when communicating with fellow students, staff, and the public.

2.2 In addition, these guidelines provide information to students to provide them with online safety advice to protect against online fraud and identity theft.

3. Scope

3.1 The scope of this guidelines is inclusive of all students who engage in interactive online media for communication and information sharing. This includes if content is text, images, video, audio, or links to other sources.

3.2 It is the responsibility of each student to adhere to these guidelines. Where inappropriate use of social media may constitute an offence under criminal law, referral will be made to the appropriate authorities. In addition, students in breach of these guidelines could find themselves in breach of the following college policies:

IT Acceptable Use Policy
IT BYOD Policy
Student Equality, Diversity and Inclusion Policy
Student Anti-bullying and Harassment Policy
Student Sexual Misconduct Policy
Student Disciplinary Policy
Safeguarding Policy

4. Use of social media at NMITE

4.1 NMITE encourages students to make reasonable and appropriate use of social media as part of their studies. Students have responsibility for their personal use of social media and where this may impact on their peers, members of staff, the reputation of NMITE and the wider community. When using social media; students should use the same safeguards as they would with any other form of communication.

4.2 Students may also have access to NMITE social media sites. All social media accounts run on behalf of NMITE are set up by the Digital Team so that NMITE maintains a log of the social media accounts they operate.

4.3 Students should be aware that that everything they post online will be public and permanent, regardless of the privacy settings applied. In addition, social media content may easily become available to the public, including NMITE staff and the media, and that inappropriate use could result in criminal or internal disciplinary proceedings, damage to reputation and future career prospects.

4.4 Student should endeavor to follow the online safety guidance in Section 6, to help protect themselves and NMITE from being at risk from criminal activity, including malware, online fraud and identify theft.

5. Social Media Guidelines

5.1 Students should respect the dignity and privacy of others and should always consider how their online behaviour may affect other people.

5.2 Students must not do anything that could be considered discriminatory against, or the bullying or harassment of any individual, for example by:

i. making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age

ii. using social media to bully, harass or intimidate another individual such as students, staff, or members of the public.

iii. posting images that are discriminatory or offensive (or links to such content).

iv. to disseminate misleading information or share confidential or sensitive information.

v. to view or distribute sexually explicit or offensive content.

vi. to share information that could create a security risk for NMITE, its staff or students.

5.3 The above examples are by no means exhaustive and misuse or inappropriate use of social media may require a disciplinary investigation which could incur a disciplinary sanction.

5.4 Through social media platforms, students must not engage in misconduct or behaviour which brings or may bring NMITE into disrepute.

5.5 When participating in a social media site as part of their studies or as a member of NMITE, students should conduct themselves in a professional manner that fully adheres to these guidelines and related policies.

6. On-line Safety Guidelines

6.1 The NMITE IT department has implemented centralised, automated virus detection and anti-malware software updates. All NMITE PCs have antivirus software installed to detect and remove any virus and malware automatically. For further information students should refer to the IT Acceptable Use Policy.

6.2 If you access any of the NMITE services on your own personal devices you must read and adhere to the IT BYOD Policy.

6.1 **Internet Safety**

Internet safety is something everyone needs to think about when they go online.

Here's 5 top tips to think about as a minimum:

- Don't post **personal** information online - like your home address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself online - it's easy to post but not always easy to remove!
- Keep your privacy settings as high as possible (social media settings).
- **Never** give out your passwords.
- Don't befriend people online you don't know in real life.

6.2 Online Identity

Our online identity is all the information we leave on the Internet. It's our digital footprint, with such details as our email address, date of birth, bank details, and even our purchasing habits on online stores. Online identity goes beyond what we do online. It also verifies that we are who we say we are. Use this link to find out more.

Identity theft refers to a crime committed to obtain personal information such as passwords, ID numbers, credit card numbers or national insurance numbers. Identity theft criminals then misuse this personal or sensitive information and act fraudulently in the victim's name, commonly to apply for loans, make an online purchase or to access the victim's medical and financial data.

The term identity fraud is sometimes used as a synonym for identity theft, although the concept of identity fraud also encompasses the use of false or modified identity, as opposed to identity theft where criminals misuse someone else's real identity.

6.3 Passwords

Passwords are used to access our online interactions, browsing and services. To help keep your passwords safe you may consider using a password manager, as a minimum follow the tips below and follow this for more information.

- Use a strong and separate password for your email.
- Install the latest software and app updates.
- Turn on 2-step verification (2SV)
- Password managers: using browsers and apps to safely store your passwords.
- Backing up your data.

- Use three random words.

6.4 Email Security

Students should remain alert to the security threat from phishing emails.

These are generally designed to try and steal your online credentials by getting you to click on a link or open an attachment. They normally masquerade as an email from your bank, student loan company, Inland Revenue or the police but could be an online shopping site or streaming media company. They can be very convincing. Click this link to find out more!

The general rules are:

- If in any doubt at all about the origin or authenticity of an email – simply delete it.
- Hover over links before clicking them – sometimes this will show the underlying link is NOT to where you think!
- Unless you're sure an email is genuine, do NOT click on links it contains.
- And DON'T enter credentials or passwords into a website accessed from a link you've got any doubts about
- Please alert IT Support immediately via the Service desk on MyNMITE, if you think you have done one of these. We don't judge, we just need to check things ASAP.

7. How to report concerns

7.1 If you have any concerns or doubts about your online safety, you should report this immediately to the IT Service Desk – accessed via MyNMITE. In addition, if your concerns are around bullying and/or harassment or potential criminal activity you can speak to the Student Services Team who can support you to report to the appropriate authorities.

Appendix 1 – Social Media Platforms

Type	Social Media Platforms	Purpose
Audio Platforms	Clubhouse, Twitter Spaces, Spotify	Listen to live conversations on specific topics
Video Platforms	YouTube, TikTok, Instagram Stories and Reels, Facebook Watch	Watch videos in short and long formats
Disappearing Content	Snapchat, Instagram Stories, Facebook Stories, LinkedIn Stories	and publish conveniently, at-the-moment content for all your followers that lasts for 24 hours
Messaging Platforms	WhatsApp, telegram, Discord, Threads. MS Teams	To stay connected and send quick messages privately
Discussion Forums	Reddit, Quora	Debate and discuss, network, form communities around a subject, and share views on internet-driven topics
Shoppable Social Media Platforms	Pinterest Product Pins, Facebook Shops/Marketplace, Instagram Shops, TikTok, Shopify,	Research and purchase products directly from companies through social media platforms
Live Streams	Twitch, YouTube, Instagram Live Rooms, Facebook Live, TikTok	Broadcast live video to viewers. This ranges from a person broadcasting what they're doing on the screen to ethically organized conferences with numerous speakers
Business Platforms	LinkedIn, Twitter, MS Teams	Collaborate with professionals in your niche or with potential clients

Closed/ Private Community Platforms	Discourse, Slack, Facebook Groups, Meetup, InterNations	Forming communities, you should register or use other screening measures for new members.
Inspirational Platforms	Pinterest, YouTube, Instagram, blogs	Surf for information and find inspiration for anything from food to travel to shopping and more

Policy Owner	Director of Registry and Student Life	
Version Number	5.0	
Date Policy (Re)Approved	07/2025	
Approval authority	Safeguarding Panel	
Date of Commencement	08/2025	
Equality Impact Assessment (EIA) completed	04/2025	
Amendment History	Date	Reason for Update
	08/2023	Annual review
	08/2025	Biennial Review
Summary of changes made to this version	None	
Date for next review	01/08/2027	
Related Policies, Procedures, Guidance, Forms or Templates	IT Acceptable Use Policy IT BYOD Policy Student Equality, Diversity and Dignity Policy Student Anti-bullying and Harassment Policy Student Sexual Misconduct Policy Student Disciplinary Policy Safeguarding Policy	
Policies superseded by this Policy	V1:Feb2020 V2:Aug2021 V3: Aug2022 V4: Aug 2023	