

Version Control Statement

ID Number:	FW045	Document Name:	Student_Social_Media_Policy_V1.5.0
Approving Committee:	Operations Team		
Last Review:	August 2025	Next Review:	Mar-28 to May-28
Owner:	Vice Principal	Review Lead:	Head of Student Affairs
Amendments Since Approval:	Detail of Revision:	Date of Revision:	Revision Approved by:
	New social media channels added in section 5		
	New legislation which has come into place since the last review added in section 11		
	Executive Team changed to Operations Team	10/09/24	Operations Team
	Minor changes to language and grammar, update to legislative documents, update to social media platforms, update to roles and contact details.	01/09/25	Operations Team

Student Social Media Policy

1. Introduction

Social media has created increased opportunity for communications that have an impact on Futureworks both as a collaboration tool for teaching, learning and research, and for interactions with students, parents, alumni and the business and wider community. Futureworks has clear policies and guidelines for other aspects of its operations however, these do not explicitly cover the use of social media by students. This Policy has been compiled to help students understand the reputational, legal and ethical implications of engaging in on-line communication of this nature – and what can happen if social media is misused, whether intentionally or otherwise.

2. Relevant Legislation & Futureworks Policies

This Policy does not sit in isolation. Students should be aware that a number of other relevant policies and guidelines exist, which are relevant to conduct while using social media. Certain conduct may be regarded as misconduct in terms of the provisions of the following, including but not limited to Futureworks’:

- Academic Freedom and Freedom of Speech Policy.
- Approval of Published Information Policy.
- Equality & Diversity Policy.
- Student Code of Conduct.
- Safeguarding Policy.
- Ethical Practice Policy.
- Statutory regulations, such as:
 - Section 26 of the Counter-Terrorism and Security Act 2015 (the Prevent Duty)
 - General Data Protection Regulation (GDPR)
 - Equality Act (2010)
 - Human Rights Act (1998).
 - Online Safety Act (2023)

3. Statement of Intent

Futureworks embraces the evolution and use of social media as a tool of communication and collaboration in both the creative industries and higher education. Given that social media affords students a public platform to express themselves, it is important that clear guidelines

regarding responsible behaviour, standards of conduct and expectations that users must adhere to when using social media are established.

4. Objectives

The objectives of this Policy are to:

- Provide a definition of relevant terms and articulate the potential risks social media misuse poses to Futureworks, its staff and students.
- Identify the types of activity that this Policy applies to.
- Define students' social media responsibilities.
- Coordinate and oversee the response to misuse in accordance with the requirements of UK legislation and Futureworks policies & procedures.
- Minimise the potential negative impact to Futureworks, its stakeholders and third parties as a result of incidents and violations.

5. Definitions and Risks

Social media is any website or medium that allows for public communication, including (but not limited to) social and professional networking sites, blogs, micro-blogging sites, video and photo-sharing sites, forums, discussion boards and groups, podcasting sites and instant messaging services (including short messaging services (SMSs)), whether accessed using the Futureworks IT facilities and equipment, or equipment belonging to members of staff or any other third party. Examples of popular social media sites include, but are not limited to:

- | | |
|--------------|---------------------------------|
| • ArtStation | • Soundcloud |
| • Ask.fm | • Skype |
| • Cubebrush | • Threads |
| • Discord | • TikTokTumblr |
| • Facebook | • Twitch |
| • Flickr | • Vimeo |
| • Instagram | • Viva Engage (formerly Yammer) |
| • LinkedIn | • Wiki's/Blogs |
| • MySpace | • YouTube |
| • Pinterest | • X (formerly known as Twitter) |
| • Reddit | |
| • Snapchat | |

(Content from private messaging platforms such as WhatsApp or Facebook Messenger will fall under the remit of this policy if Futureworks receives a complaint regarding content.)

Bullying is defined, as unfair treatment, excessive criticism, or persistent nitpicking, intimidating, aggressive or undermining behaviour, which makes the recipient(s) feel upset, humiliated, threatened or vulnerable and undermines their self-confidence and integrity.

Cyberbullying is the use of the Internet and related technologies to harm or harass other people, in a deliberate, repeated, and hostile manner.

Extremist/terrorist content is defined as material that supports, directs or glorifies: terrorism; serious violence against a person; serious damage to property; endangering a person's life; creating a serious risk to the health or safety of the public or a section of the public; or is designed seriously to interfere with or seriously disrupt an electronic system and is designed to intimidate the public or a section of the public or influence the government or an international

organisation for the purpose of advancing a political, religious, racial or ideological cause. This content can take the following forms, including but not limited to:

- Speeches or essays calling for racial or religious violence.
- Videos of violence with messages in praise of terrorists.
- Postings inciting people to commit acts of terrorism or violent extremism.
- Messages intended to stir up hatred against any religious or ethnic group.
- Bomb-making instructions.
- Advice on how to obtain or make weapons.
- Articles, images and/or videos that promote terrorism or encourage violence.
- Websites made by terrorist or extremist organisations.

Harassment is unwanted conduct based on the grounds of religious belief, political opinion, sex (including gender reassignment, marital or civil partnership status), race/ethnicity, disability, sexual orientation or age which has the purpose or effect of violating that person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person. Differences of attitude, background or culture and the misinterpretation of social signals can mean that what is perceived as harassment by one person may not seem so to another; nevertheless, this does not make it acceptable. It is the purpose or effect of the behaviour rather than the motive that must be considered.

All students using social media tools, including via personal accounts, must be aware that principles of integrity, professionalism, privacy and impartiality should be observed when posting on-line. Any official Futureworks position or comment must be approved by the Vice-Principal or their representative. The potential risks associated with the misuse of social media include, inter alia:

- | | |
|--------------------------|---|
| • Reputational damage | • Publication of inaccurate, misleading and/or inappropriate information |
| • Breach of confidence | • Violation of applicable laws such as data protection, copyright, trademark, defamation, |
| • Breach of data/privacy | • Hacking, phishing and malicious attacks |
| • Legal actions | • Radicalisation/terrorism |
| • Safeguarding incidents | |
| • Disciplinary actions | |
| • Extremist grooming | |

6. Student Responsibilities

It is the responsibility of students to read and act in accordance with the principles of this Policy. Social media must only be used in ways that do not breach Futureworks policies & procedures, statutory duties and other regulations. Students should be aware that breaches of these policies, duties and regulations may affect progression to the next level of study, and may affect professional suitability. Employers make no distinction between using social media in a personal capacity and as a Futureworks student. Inappropriate postings/use of social media may affect your ability to find work upon graduation. Students are responsible for ensuring that passwords and other access controls for Futureworks social media accounts are of adequate strength, kept secure and must not be shared under any circumstances. Passwords should be changed regularly. Students should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience.

7. Responsibilities of students using official Futureworks on-line/social media presence

The Futureworks logo should be used on official Futureworks on-line channels, such as the VLE and on-line channels established by Student Partners. Students should be aware that they are representing Futureworks when posting comments, liking, sharing or responding to comments

made by others on social media. Any communication by a Futureworks student made through social media must **not**, among other things:

- Do anything that could be considered discriminatory against, or bullying or harassing of, any individual e.g. making offensive or derogatory comments relating to sex, gender, race (including nationality), disability, sexual orientation, religion or belief or age.
- Contain images or other content that is sexually explicit or illegal.
- Contain extremist/terrorist content and/or radicalise and recruit vulnerable people.
- Bring discredit to Futureworks in any way e.g. by insulting fellow students or other individuals; making/sharing defamatory or offensive comments about individuals or groups; liking/posting/ sharing/linking to images or other content that is inappropriate, sexually explicit or illegal.
- Breach copyright, e.g. by using someone else's images or content without permission, or by failing to give acknowledgement where permission has been given to reproduce. This means, for example, not posting articles or pictures scanned from newspapers or magazines. Posting such content may result in legal action by the copyright owner.
- Breach confidentiality, for example, by revealing confidential information owned by Futureworks; posting confidential information about an individual, business or other organisation; posting contact details, pictures or personal details of other students or members of staff or members of the public without their prior written permission. Students must seek prior advice from the Academic Registrar via dataprotection@futureworks.ac.uk if unclear about what information might be deemed confidential.

If there is any doubt about the accuracy of information to be shared on a social media network or site then, students should refrain from posting, commenting, liking or sharing this information. For guidance on using the Futureworks branding/logo, contact liaison@futureworks.ac.uk

8. Responsibilities of students using personal on-line/social media presence

Students are personally responsible for content they post or share via social media. It is essential that students respect the privacy and the feelings of others at all times, and understand that the content posted via social media is a permanent record which is shared instantaneously with a potential global audience. Students must not use the Futureworks logo on personal social media sites or other websites. A student's personal on-line or social media profile may identify Futureworks as their place of study, but it must be made be clear that comments/posts/shares made by the account holder are made in a personal capacity only. Students should include a simple and visible disclaimer for clarity such as: "The views I express are mine alone and do not reflect the views of my place of study".

9. Monitoring, Reporting & Complaints

Futureworks will monitor official Futureworks social media sites, and we reserve the right to request the removal of any content deemed to be in breach of this policy. We also monitor references to Futureworks on-line and will act, where necessary to protect our reputation. Futureworks will refer to social media sites when investigating breaches or complaints under this Policy. Any misuse or any use that may bring Futureworks or one of its staff/students into disrepute must be reported to the Academic Registrar e, via dataprotection@futureworks.ac.uk in the first instance.

Complaints concerning the misuse of social media by Futureworks students will be dealt with using the procedures set out in the Student Complaints Process.

Where a complaint involves threatening or potentially criminal social media behaviour, the matter will also be reported to the Greater Manchester Police for investigation. This will include, but is not limited to, complaints in which a student is alleged to have, among other things:

- Posted on-line photos or videos of people in a place where he or she would expect privacy.
- Threatened violence.
- Accessed or shared child pornography.
- Sent sexually explicit images or photos.
- Engaged in stalking.
- Committed a hate crime.

10. Communication & Training

All students will receive this information by way of the Futureworks Student Policies and Procedures Handbook, which is discussed in depth during induction.

11.

12. Further Information

- The use of social media for on-line radicalisation (Ref. DfE and HO 2015): <https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation>
- Proscribed terrorist groups or organisations (Ref. HO 2017): Updated 24 April 2024 <https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version>
- The Online Safety Bill (2022): <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>

The Online Safety Act (2023): <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>

13. Social media hints and tips

- **Do:**
 - Check with your personal tutor before publishing content that may have controversial implications for the institution.
 - Use a disclaimer when expressing personal views, clarifying that the views expressed are personal and not those of Futureworks.
 - Make it clear who is posting content and in what capacity.
 - Use an appropriate, professional tone and avoid any sort of discriminatory, inflammatory or defamatory language.
 - Be respectful to all parties.
 - Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
 - Express opinions but do so in a balanced and measured manner, using your best judgement.
 - Manage your social media presence when this is on behalf of or could be viewed as being on behalf of Futureworks, avoiding bringing the Futureworks into disrepute.
 - Think before responding to comments and, when in doubt, get a second opinion.
 - Seek advice and report any mistakes to the Data Protection Officer via: dataprotection@futureworks.ac.uk
 - Use common sense.
 - Check the accuracy of your posts, comments or replies



- If you believe anyone to be a victim of harassment or bullying online, report it to the Data Protection Officer via dataprotection@futureworks.ac.uk immediately.
- Don't:
 - Make comments, post content or link to materials that will bring the Futureworks into disrepute.
 - Publish extremist/terrorist content and/or radicalise and recruit vulnerable people.
 - Use the Futureworks logo/branding on personal accounts.
 - Publish confidential or commercially sensitive material.
 - Publish personal information not relating to you without written consent.
 - Breach copyright, data protection or other relevant legislation.
 - Link to, embed or add potentially inappropriate content and consider the appropriateness of content given the age and capacity of the learners.
 - Post derogatory, defamatory, inflammatory, offensive, harassing or discriminatory content.
 - Use the Futureworks brand or name to endorse any view, cause, product, private business or political cause
 - Use social media to air grievances of any kind or make people feel uncomfortable.
 - Do anything illegal or dangerous.