OZFORD
Institute of Higher Education

SOCIAL MEDIA POLICY (STAFF)

Approving authority	Governing Board
Purpose	This Policy provides the Institute's staff with guidelines for the appropriate use of media and social media.
Responsible Officer	President and CEO
Next scheduled review	**February 2031**
Document Location	https://www.ozford.edu.au/policies-and-procedures/higher-education/
Associated documents	Academic Integrity Policy and Procedure Anti-Bullying and Harassment Policy and Procedure Anti-Discrimination Policy and Procedure Diversity and Equity Policy and Procedure Engaging Managing and Monitoring the Performance of Education Agents Policy and Procedure Human Resources Policy and Procedure (Manual) Marketing and Advertising Materials Policy and Procedure Occupational Health and Safety Policy Privacy Policy and Procedure Records Management Policy and Procedure Sexual Assault and Sexual Harassment Policy and Procedure Staff Code of Conduct Policy and Procedure Use of Information Technology Facilities and Services Policy and Procedure (Staff) Social Media Procedure (Staff) Employment agreement

1. PRINCIPLES

Ozford Institute of Higher Education (herein after referred to as 'the Institute') recognises the importance of social media as a communication tool that is regularly used by its staff, students and associates to connect with each other and the broader community. Accordingly, and in recognition of the rapid growth and application of social media, the Institute has recognised the need for a policy to ensure that those who use these media as part of their professional role, in a personal capacity, study or association with the Institute do so consistent with Institute guidelines for acceptable use.

The following five principles apply to the use of social media for Institute staff and students:

- show respect for human dignity and adhere to the Institute Mission and values;

- do not use social media to bring Institute, staff or students into disrepute;
- do not imply Institute endorsement of personal views;
- ensure confidentiality of information obtained through the Institute is maintained; and
- do not use social media to the detriment of Institute academic and professional activities.

This policy includes all social media sites and covers all future social media systems and access to social media by any means including via computer, tablet, mobile phone, handheld or wearable device.

2. SCOPE

This policy sets out the Institute's expectations for the use of social media by Institute staff for educational, Institute business and personal use purposes where they can be identified as the Institute staff.

This policy does not apply to use of ICT facilities and services. Staff should instead refer to the ***Use of Information Technology Facilities and Services Policy and Procedure (Staff)***.

3. DEFINITIONS

Identifiable Personal Use

'Identifiable Personal Use' is defined as the use of social media where a student can be identified as being enrolled at the Institute through means including but not limited to the person's social media name, character, profile or comments.

Institute Environments

Institute environments means any physical or virtual place made available by the Institute for teaching, learning or Institute activities, including:

- the campus;
- Online learning environments; and
- Other physical environments where the Institute operates or conducts activities.

Physical environments are the physical places where an organisation operates or conducts activities, such as a building, facility or space and includes physical environments operated by third parties.

Online environments are any technological platforms which an organisation uses or controls, such as computers, phones, websites, intranet, email, social media and video conference facilities regardless of where such platforms may be accessed by students.

Media

Any organisation that publishes material for consumption by the general public or specific interest groups, including print, radio, television and online. Media organisations include those that are publicly and privately owned, run by volunteer organisations, including students, and have an international, national or local focus.

Post

Post in this policy refers to any shared or created content put on social media. This could be a post on social media, a message in an App or content created and edited on Wikipedia.

Severe or serious misconduct

Serious misconduct includes but not limited to

- Acting dishonestly including any fraud in respect to the Institute, students or stakeholders;
- Knowingly making any false or misleading representation;
- Harassing or intimidating a student, a member of staff, a visitor to the Institute, or any other person, because of race, ethnic or national origin, sex, marital status, sexual preference, disability, age, political conviction, religious belief or for any other reason;
- Misuse of the facility in a manner which is illegal, or which is or will be detrimental to the rights or property of others. This includes the misuse, in any way, of any computing or communications equipment or capacity to which the employee has access at or away from the Institute premises while acting as an Institute employee, in a manner which is illegal, or which is or will be detrimental to the rights or property of others;
- Theft or an action to steal, destroy or damage a facility or property of the Institute or for which the Institute is responsible.
- Any form of physical violence against a student, staff member or stakeholder of the Institute that is substantiated;
- A child abuse incident where the allegation is substantiated; or
- Being under the influence of alcohol or drug of dependence during working hours.

Social Media

Social media are online media designed to allow information to be shared, disseminated and created using highly accessible and scalable publishing techniques. This policy applies to all social media including but not limited to:

- social networking sites: Facebook, Instagram, Google+, Foursquare, LinkedIn;
- any other official and unofficial pages on social and professional networking sites that are set up by individuals, groups, clubs and societies;
- video and photo sharing websites: YouTube;
- micro-blogging sites: Twitter and Tumblr;
- blogs: including corporate blogs, personal blogs or blogs hosted by traditional media publications;
- vodcasting and podcasting sites: including corporate podcasts and personal podcasts;
- forums and discussion boards: e.g. local discussion boards, Whirlpool, Yahoo! Google Groups;
- online multiplayer gaming platforms: e.g. Second Life;
- blogs hosted by media outlets (e.g. 'comments' or 'your say' feature on theage.com.au);
- sharing economy websites, such as Gumtree and Uber
- instant messaging including SMS, Wechat, Line and Kakao Talk.

4. POLICY

Use of Media and Social Media

4.1 The Institute encourages the use of social media as an effective complementary teaching strategy to practice critical thinking and problem-solving skills in collaborative environments. The Institute acknowledges the positive impact that the use of social media in learning and teaching can make to student engagement and experience, active learning, digital literacy and citizenship.

4.2 Freedom of speech and academic freedom are defining values of the Institute. Media, social media and communications activity by staff is supported by the Institute's ***Free Intellectual Enquiry in Learning and Teaching Policy.***

4.3 Use of media or social media must adhere to the conduct expected of staff outlined in this Policy and the:

- ***Staff Code of Conduct Policy and Procedure***
- ***Academic Integrity Policy and Procedure***
- ***Anti-Bullying and Harassment Policy and Procedure***
- ***Anti-Discrimination Policy and Procedure***
- ***Diversity and Equity Policy and Procedure***
- ***Human Resources Policy and Procedure (Manual)***
- ***Occupational Health and Safety Policy***
- ***Privacy Policy and Procedure***
- ***Sexual Assault and Sexual Harassment Policy and Procedure***
- ***Use of Information Technology Facilities and Services Policy and Procedure (Staff)***

4.4 Personal, academic and professional use of social media by staff must not:

- include content that is misleading or inaccurate;
- interfere with a staff member's duties or a student's studies;
- bring the Institute into disrepute;
- compromise the effectiveness of the Institute;
- defame individuals or organisations;
- use the Institute's name or brand artefacts (including crest or logo) in the account name or profile without approval;
- imply the Institute endorsement of personal views; or
- disclose, without authorisation, confidential information.

4.5 When accessing internal social media networks, staff must use the Institute's ICT facilities and services in an acceptable manner. This should not interfere with the performance of their work.

4.6 In addition to this, when using social media at work, staff must:

- be polite and respectful of the opinions of others at all times;
- be mindful that others may not share the same sense of humour;

- not use the Institute's ICT resources to provide comments to journalists, politicians or lobby groups other than as approved by the Vice-president;
- not access or engage with any material that is inappropriate or unlawful. This may include posts that are fraudulent, threatening, bullying, embarrassing, of a sexual nature, obscene, racist, sexist, defamatory or profane, whether obscured by symbols or not;
- not use the Institute's ICT resources to post explicit or sexually suggestive messages;
- not infringe another person's, or the Institute's, privacy or intellectual property rights.
- report issues and any cyberbullying.

4.7 When using social media, it is not acceptable for staff at any time to:

- make any comment or post material that is, or might be construed to be, racial or sexual harassment, offensive, obscene (including pornography), defamatory, discriminatory towards any person, or inciting hate;
- make any comment or post material that creates, or might be construed to create, a risk to the health or safety of a fellow student, contractor, staff member or other person, including material that amounts to bullying, psychological or emotional violence, coercion, harassment, sexual harassment, aggressive or abusive comments or behaviour, and/or unreasonable demands or undue pressure;
- make any comment or post material that infringes privacy, copyright, is fraudulent, breaches intellectual property rights, constitutes a contempt of court, constitutes stalking, breaches a court order, or is otherwise unlawful;
- imply that the staff member is authorised to speak as a representative of the Institute or give the impression that the views they express are those of the Institute unless authorised by the Institute President and CEO to do so;
- use the identity or likeness of another student or staff member of the Institute;
- compromise academic honesty or encourage cheating or plagiarism including sell or offer to write assignments or other assessable work;
- create a social media page to protest policies that staff are responsible for implementing or promoting;
- make any comment or post material that might otherwise cause damage to the Institute's reputation or bring it into disrepute;
- use the Institute's crest or logo without permission or use the Institute's name in a manner that is likely to be misleading or bring the Institute into disrepute.
- post inappropriate images that reference or involve the Institute in some way;
- use an Institute work email address, or anything else that connects the staff member to the Institute, when making public comment that has not been authorised;
- use external social media tools for business related internal communications, this excludes approved Institute software such as SharePoint and Skype.

4.8 Staff should be mindful that their social media use in their private time can have, or can be construed as having, a connection to the Institute. Staff must ensure that their private use of social

media does not create a connection with the Institute which is, or is likely to be, detrimental to the Institute or its community. Before deciding to post something, staff must be mindful that:

- comments posted online are available immediately to a wide audience;
- material posted online effectively lasts forever and may be copied without limit;
- others may view material posted online out of context or use it for an unintended purpose;
- a site's security settings cannot be relied on to protect or keep material private;
- anything posted can be traced back and used to identify the poster as a student;
- defamation, privacy, copyright and other laws apply to media and social media; and
- anonymity or a pseudonym cannot be relied on to protect against identification.

4.9 Staff who are alleged to have misused media or social media will be subject to investigation and, if misuse is established, action will be taken as detailed in this Policy.

4.10 All breaches of this Policy will be treated seriously.

4.11 Staff who become aware of misconduct by any student or staff member particularly if they infringe the rights of another person, or that the effect of any use of any facilities is to infringe such rights, must notify the CEO and President.

4.12 The Institute will investigate the matter and if a breach is confirmed, will pursue action under the relevant Institute policy.

4.13 The outcome of a substantiated breach may include, but is not limited to the following:

- Counsel staff on appropriate media or social media use;
- Suspend or withdraw access to the email service, system access and/or network services.
- Require staff to indemnify or compensate the Institute or a provider for the reasonable loss and damage occasioned by reason of the misuse;
- If the misuse constitutes a potential breach of privacy, refer to and manage this in accordance with the ***Privacy Policy and Procedure***.
- Disciplinary action in accordance with the ***Human Resources Policy and Procedure (Manual).***

4.14 Staff can access the ***Human Resources Policy and Procedure (Manual)*** or the process set out in their Employment agreement if they are aggrieved by an Institute decision.

4.15 In addition to any disciplinary action by the Institute, a breach of this policy this may lead to civil or criminal proceedings and penalties, which the Institute may report to relevant law enforcement bodies and for which staff will be held personally accountable.

Reporting

4.16 All non-compliance with legislative requirements or serious misconduct incidents will be reported to the Audit and Risk Committee and the Governing Board.

5. QUALITY ASSURANCE

To ensure that this policy is fit for purpose and meets the requirements of the TEQSA Compliance Frameworks the Policy will be:

5.1 internally endorsed by the Executive Management Team on development or review, prior to approval by Governing Board, or other delegated authority;

5.2 externally reviewed as part of any independent review of the TEQSA Compliance Frameworks approved by the Governing Board;

5.3 internally reviewed by the Responsible Officer every five years from the date of approval (if not earlier).

5.4 referenced to the applicable TEQSA Compliance Frameworks requirement(s) and/or other legislation/regulation.

6. FEEDBACK

Feedback or comments on this policy is welcomed by Executive Management Team of the Institute or other delegated authority.

7. ACKNOWLEDGEMENT

This policy was developed with reference to the following:

- Monash University, Media and Social Media Policy, 2021 (Media and Social Media Policy (monash.edu))
- Victoria University Social Media Procedure, 2018 (https://policy.vu.edu.au/document/view.php?id=429)
- Australian Catholic University Social Media Policy, 2021 (Social Media Policy - Policies - Australian Catholic University (acu.edu.au))

8. VERSION CONTROL

Version	Date approved	Description	Approved by
1.0	June 2018	Initial Development	GB
2.0	June 2018	Minor formatting and editorial changes	GB
3.0	September 2023	Internal Review	GB
3.1	February 2026	Internal Review to remove under 18 student obligations after change in policy	EMT

Version	Date approved	Description	Approved by
Related legislation/ regulation/standard	**Commonwealth** Tertiary Education Quality and Standards Act 2011 (Cth) Higher Education Standards Framework (Threshold Standards) 2021 (Cth) Education Services for Overseas Students Act (ESOS) 2000 (Cth) Education Services for Overseas Students Regulations 2019 (Cth) The National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth) Higher Education Support Act 2003 (Cth) FEE-HELP Guidelines 2017 (Cth) Higher Education Provider Guidelines 2012 (Cth) Higher Education Support (HELP Tuition Protection Levy) Act 2020 (Cth) Higher Education (Up-front Payments Tuition Protection Levy) Act 2020 (Cth) Student Identifiers Act 2014 (Clth) Age Discrimination Act 2004 (Cth) Australian Consumer Law (Cth) Australian Human Rights Commission Act 1986 (Cth) Copyright Act 1968 (Cth) Crimes Act 1914 (Cth) Disability Discrimination Act 1992 (Cth) Disability Standards for Education 2005 (Cth) Fair Work Act 2009 (Cth) Fair Work Regulations 2009 (Cth) Privacy Act 1988 (Cth) Racial Discrimination Act 1975 (Cth) Sex Discrimination Act 1984 (Cth) Sexual Offence Crimes Act 1958 (Cth) SPAM Act 2003 (Cth) Workplace Gender Equality Act 2012 (Cth) **Victoria** Accident Compensation (Occupational Health and Safety) Act 1996 (Vic) Australian Consumer Law and Fair Trading Act 2012 (Vic)		

Version	Date approved	Description	Approved by
	Charter of Human Rights and Responsibilities Act 2006 Charter of Human Rights and Responsibilities (General) Regulations 2017 Competition and Consumer Act 2010 (Vic) Compliance Code Psychological Health (Vic) Corporations (Victoria) Act 1990 (Vic) Crimes Act 1958 (Vic) Disability Act 2006 (Vic) Equal Opportunity Act 2010 (Vic) Gender Equality Act 2020 Health Records Act 2001 (Vic), Mental Health and Wellbeing Act 2022 (Vic)Occupational Health and Safety Act 2004 (Vic) Occupational Health and Safety Regulations 2017 (Vic) Occupational Health and Safety (Psychological Health) Regulations 2025 (Vic) Privacy and Data Protection Act 2014 (Vic), Public Records Act 1973 (Vic) Racial and Religious Tolerance Act 2001 (Vic) Spent Convictions Act 2021 (Vic) **Queensland** Anti-Discrimination Act 1991 (Qld) Corporations (Administrative Actions) Act 2001 (Qld) Crime and Corruption Act 2001 (Qld) Disability Services Act 2006 (Qld) Domestic and Family Violence Protection Regulation 2023 (Qld) Domestic and Family Violence Protection Rules 2014 (Qld) Education (Work Experience) Act 1996 (Qld) Fair Trading Act 1989 (Qld) Fair Work (Commonwealth Powers) and Other Provisions Act 2009 (Qld) Health and Wellbeing Queensland Act 2019 (Qld) Holidays Act 1983 (Qld) Human Rights Act 2019 (Qld) Human Rights Regulation 2020 (Qld)		

Version	Date approved	Description	Approved by
	Information Privacy Act 2009 (Qld) Information Privacy Regulation 2025 (Qld) Work Health and Safety Act 2011 (Qld) Work Health and Safety Regulation 2011 (Qld) Work Health and Safety and Other Legislation Amendment Act 2024 (Qld)		

Note:

GB = Governing Board

EMT = Executive Management team