SOCIAL MEDIA PROCEDURE (STAFF)

Approving authority	Executive Management Team
Purpose	This procedure provides the Institute's staff with guidelines for the appropriate use of media and social media.
Responsible Officer	President and CEO
Next scheduled review	August 2026
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	Social Media Policy (Staff) Academic Integrity Policy and Procedure Anti-Bullying and Harassment Policy and Procedure Anti-Discrimination Policy and Procedure Child Safety 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)

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 procedure 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 procedure 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 procedure 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 use by a child 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 such as student advocates and homestay accommodation.

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 Facebook, a message in Skype 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, Skype, Wechat, Line and Kakao Talk.

4.   PROCEDURE

Use of Media and Social Media

4.1   Staff are informed about the **Social Media Policy and Procedure (Staff)** during induction. For staff who will have a role using media and social media, the Head of Department will provide on the job training.

4.2   The Institute provides its staff with access to ICT facilities and services to assist and support its teaching, learning, research and administrative activities.

4.3   Staff using social media are required to do so in compliance with the **Social Media Policy (Staff)**, this Procedure and the following policies and procedures:
- **Staff Code of Conduct Policy and Procedure**
- **Academic Integrity Policy and Procedure**
- **Anti-Bullying and Harassment Policy and Procedure**

- **Anti-Discrimination Policy and Procedure**
- **Child Safety 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   The use of social media by Institute staff is subject to these procedures in each of the following circumstances:
- If the social media site is established or used as an Institute social media site, including for education, research and/or any collaboration purposes;
- If the content of the social media is specifically about the Institute or its staff or students, in whole or in part; and/or
- If a person identifies themselves as being associated with the Institute (e.g. as a staff member).

Institute media and social media

4.5   Staff must observe the following before creating a social media presence that has a connection with the Institute.

4.6   The following staff are authorised to act as spokespeople for the Institute and provide a representative institutional voice in terms of content and comment on media and social media:
- Governing Board chair; or
- President and CEO.

4.7   Any social media site that staff intend to use to represent the Institute must be formally approved by the President and CEO and it must be clearly stated that the site is maintained by the Institute, have Institute contact information prominently displayed and comply with all legislative requirements.

4.8   Communications to staff and students regarding marketing and general matters such as events and class times can be made via social media channels by staff authorised by the President and CEO with prior approval of content.

4.9   Staff representing the Institute in a professional capacity in media or social media must conduct themselves in a professional and appropriate way at all times and in accordance with all relevant and applicable Institute policies.

4.10   The Institute reserves the right to restrict or remove any media or social media content that is deemed in violation of these Procedures.

Expert Comment

4.11 The Institute recognises and protects the concept and practice of freedom of opinion and expression as essential to the proper conduct of teaching, research and the pursuit of scholarship. This right carries with it an obligation for staff to use the freedom in a manner consistent with a responsible and honest search for knowledge and truth, grounded in scholarly evidence.

4.12 Institute academics who are considered expert within a particular field related to their Institute appointment are encouraged to engage in all media channels, including social media, particularly when news or social interest in the public domain has made their area of expertise topical and there is opportunity to make a valuable contribution to community discussion.

4.13 In this situation staff members may use the Institute's name and their position title (as reflected in their employment contract) to establish their credentials.

4.14 The **Social Media Policy (Staff)** and this procedure does not restrict the right of a staff member to freely express opinions in their private capacity as an individual member of society, but statements made in this context should not include the Institute's name, or the title of the person's appointment.

Monitoring and reporting issues in Media or Social Media

4.15 If a significant issue arises within media or social media, particularly one affecting or implicating the Institute or its staff or students, the following steps are recommended:
- contact the Head of Department and CEO and President to advise that an issue with media or social media has arisen;
- identify the level of issue, those involved in discussing the issue, the forums used and the extent of the commentary along with any legal ramifications;
- review and follow the conversations to establish a clear and current understanding of what is being discussed;
- assess commentary for accuracy, the risk of defamation and other legal issues, reputation risk and potential organisational sensitivities;
- if a sensitive or negative issue is being discussed in a public or social media forum, staff should always wait before responding so as to ensure the authorised spokesperson responds with an Institute approved consistent message that ensures any sensitivities and legal issues are appropriately considered.

4.16 Social media can be an extremely effective tool for dealing with crisis management in order to communicate swiftly and to a large network at short notice, and authorised spokespeople will engage with Institute official social media in the event of a crisis.

Use of images and / or video

4.17 Prior permission must be obtained to post, share or distribute images of individuals whose images are identifiable.

4.18 Staff should not post content that might be embarrassing to an individual; could be construed as placing an individual in a negative or false light or might cause someone to believe that his/her name, image, likeness or other identifying aspect of his/her identity is being used without permission for unauthorised purposes.

4.19 Most images and videos are subject to copyright and occasionally trademark, design and other intellectual property protection. Staff should verify that their use of images and/or video is:
- covered by a relevant exception for teaching or research; or
- falls within explicit licence terms of the image or video; or
- that staff have received copyright permission (as distinct from privacy clearance) to use the image or video in the way they propose.

Best practice social media guidelines

4.20 For a successful social media presence, staff should:
- **Be accurate and timely:** provide accurate information on time as this is expected from the audience, and not publish misleading information;
- **Be respectful:** be professional and respectful at all times as this can directly reflect on the individual posting the message and/or the Institute;
- **Follow:** the conversations to maintain a clear and current understanding of what is relevant and of interest to the community;
- **Recognise that online content can and will live forever:** be aware that the Internet is not anonymous and acts as a permanent record. Everything written on the web may be traced back to its author even after it has been deleted;
- **Recognise that staff cannot separate the personal from the professional:** there is no clear line between a staff member's work life and personal life. One should always be careful, honest and respectful in both capacities;
- **Avoid hazardous materials:** refrain from posting or linking to any materials that are defamatory, threatening, harassing, indecent, discriminatory, infringe copyright, constitute a contempt of court, or are otherwise unlawful;
- **Keep confidentiality:** refrain from posting any confidential or proprietary information;
- **Be aware of privacy obligations:** these should always be considered prior to posting information on any forum of social media especially if the identity of an individual can be ascertained from the information provided. In particular, personal information gained through employment with the Institute should not be posted in social media;
- **Identify, if appropriate:** when relevant, staff members or associates should identify their affiliation with the Institute and their area of specialisation.

Breach of Social Media Use

4.21 All breaches of the ***Social Media Policy (Staff)*** and this procedure will be treated seriously.

4.22 Any person concerned about the conduct of staff using social media may report their concern to the President and CEO.

4.23 The CEO and President or their delegate will investigate the matter and if a breach is confirmed, will pursue action under the relevant Institute policy.

4.24 Where required by the Institute, staff are expected to remove, and cooperate with all attempts to remove any comment, post or other online content where the Institute forms the view that it is in breach of these procedures or any other Institute policy.

4.25 Staff who fail to act on such a requirement will be in breach of these procedures and this will result in disciplinary action as set out in the **Human Resources Policy and Procedure (Manual)**.

4.26 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.

4.27 In addition to any disciplinary action by the Institute, staff must report illegal activities to relevant law enforcement bodies and the student will be held personally accountable.

Reporting

4.28 The Executive Management team will report non-compliance with legislative requirements or serious misconduct incidents to the Audit and Risk Committee and the Governing Board.

5. QUALITY ASSURANCE

To ensure that this procedure is fit for purpose and meets the requirements of the HES Threshold Standards the policy will be:

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

5.2 externally reviewed as part of any independent review of the HES Threshold Standards approved by the Governing Board;

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

5.4 referenced to the applicable HES threshold Standard and/or other legislation/regulation.

6. FEEDBACK

Feedback or comments on this procedure is welcomed by Executive Management Team of the Institute.

7. ACKNOWLEDGEMENT

This procedure was developed with reference to the following:

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

8.   VERSION CONTROL

Version	Date approved	Description	Approved by
2.0	June 2018	Initial Issue	EMT
3.0	August 2023	Internal Review	EMT
Related legislation/ regulation/standard	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) Victorian Child Safe Standards Occupational Health and Safety Act 2004 (Vic) Racial Discrimination Act 1975 (Cth) Sex Discrimination Act 1984 (Cth) Disability Discrimination Act 1992 (Cth) Disability Standards for Education 2005 (Cth) Australian Human Rights Commission Act 1986 (Cth) Workplace Gender Equality Act 2012 (Cth) Age Discrimination Act 2004 (Cth) Fair Work Act 2009 (Cth) Equal Opportunity Act 2010 Racial and Religious Tolerance Act 2001 (Vic) Spent Convictions Act 2021 SPAM Act 2003 (Cth) Copyright Act 1968 (Cth) Privacy Act 1988 (Cth) Privacy and Data Protection Act 2014 (Vic), Health Records Act 2001 (Vic), Australian Consumer Law (Cth)		

Note: EMT = Executive Management Team