

A low-angle, upward-looking shot of a diverse group of young adults gathered around, all looking at their smartphones. The phones are in various colors: yellow, pink, red, blue, and white. The background is a bright, cloudy sky. The overall mood is one of social connection and digital engagement.

Social Media and ICT Policy

Table of Contents

Organisation Statement	2
Who does this policy apply to?	3
Where does this policy apply?	4
Distribution of this policy	5
Use of the ICT systems	6
Privacy and monitoring of the ICT systems	7
What is social media?	8
Professional use of social media	9
Personal use of social media	10
How can I report breaches of this policy?	11
Confidentiality and Victimisation	12
What will happen if I breach this policy?	13



Organisation Statement

The Organisation recognises that social media and information communication technology (**ICT**) are essential tools for operational efficiency and strengthening our engagement with our community. The responsible use of these tools enhances our reputation, supports collaboration, and contributes to a positive and professional workplace culture.

This policy establishes clear standards and expectations for all workers when using social media (whether in a professional or personal capacity) and when accessing or using the Organisation's ICT systems.

The objectives of this policy are to:

- ensure the appropriate, safe, and responsible use of social media and the Organisation's ICT systems;
- provide clear guidance to workers on acceptable and unacceptable conduct in digital environments;
- support workers to engage with digital tools confidently while upholding professional standards; and
- provide a clear process for reporting breaches of this policy.



Who does this policy apply to?

This policy applies to all workers in the workplace.

For the purposes of this policy, 'workers' shall include:

every employee of the Organisation

volunteers

work experience students

contractors/subcontractors and any
of their employees whilst engaged
on work for the Organisation

consultants or consultants' employees
whilst engaged on work for the Organisation

agents whilst acting on behalf of the Organisation

Where does this policy apply?

This policy applies to conduct on social media and use of the Organisation’s ICT systems.

For the purposes of this policy, ‘conduct’ shall mean:

- reacts
- comments
- replies
- likes
- posts
- stories
- captions
- live streams

For the purposes of this policy, ‘ICT systems’ shall mean

- internet
- servers
- intranet
- email
- physical electronic devices such as computers, laptops, and mobile devices

Distribution of this policy

This policy will be made available online. All workers will be made aware of any amendments to the policy.

The policy will form part of the induction of new employees and will be provided to all other workers who perform work for the Organisation.

Use of the ICT systems

attempt to use another worker's email, use another worker's password, access another worker's files, or retrieve any stored communication unless appropriately authorised to do so

utilise the Organisation's ICT systems during working hours for social networking unless authorised to do so for business purposes

use the Organisation's ICT systems to access, send or post material that:

- is offensive, obscene, pornographic, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, or sexist;
- is illegal, unlawful, or inappropriate;
- affects the performance of, or causes damage to, the Organisation's electronic system in any way; or
- in any other way inconsistent with the standard of acceptable workplace conduct in the Organisation's policies

A worker must not



infringe on intellectual property rights when obtaining information over the ICT systems

illegally download, upload, copy, or distribute copyrighted works

use the Organisation's ICT systems for excess personal use that:

- consumes a significant amount of computing resource;
- interferes with the performance of the worker's job or other responsibilities;
- interferes with another worker's work;
- interferes with the computing activity of other users; or
- violates applicable laws, rules, policies, contracts, or licenses

use the ICT systems in an unlawful manner, or for unlawful, unauthorised, or inappropriate purposes, or for using such systems in a manner that violates Commonwealth or State law or any of the Organisation's policies and procedures, contracts, or licenses

Privacy and monitoring of the ICT systems

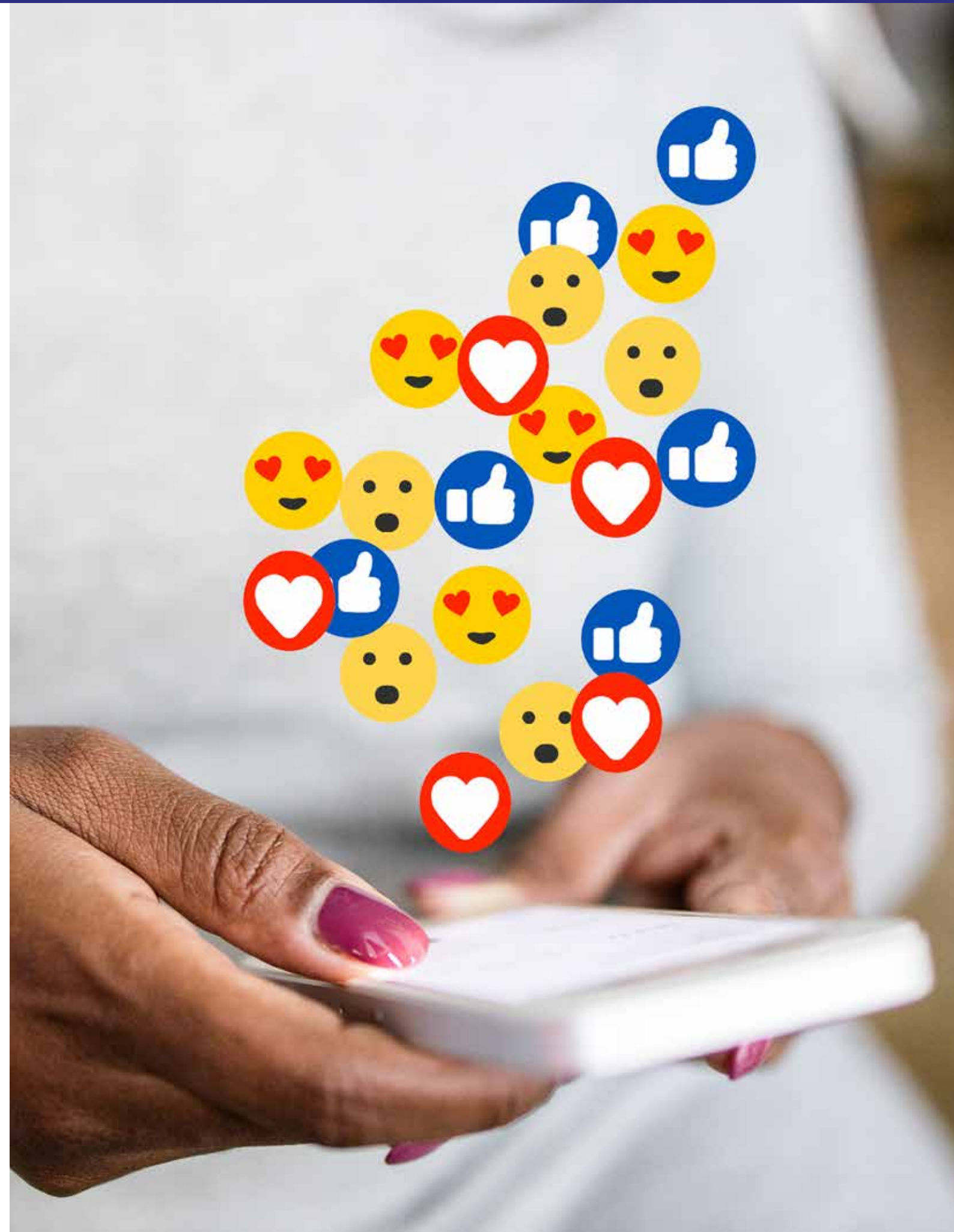
The Organisation may monitor the use of the ICT systems in order to ensure that the Organisation's property is being used appropriately.

What is social media?

Social media are websites and applications that enable users to create, access, and share public content or enables them to participate in social networking.

Social media includes (although is not limited to):

- social networking applications (eg. Facebook, LinkedIn, Yammer, Snapchat);
- video and photo sharing applications (eg. TikTok, Instagram, YouTube, Pinterest);
- blogs, including corporate blogs and personal blogs;
- blogs hosted by media outlets (eg. comments feature);
- micro-blogging (eg. X);
- wikis and online collaborations (eg. Wikipedia);
- forums, discussion boards, and groups (eg. Reddit, Whirlpool);
- instant messaging (eg. WhatsApp, Viber);
- geo-spatial tagging (eg. Foursquare, Yelp); and
- podcasting.



Professional use of social media

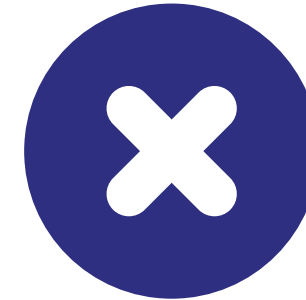
A worker must be authorised by the Organisation before making any comments or engaging in social media as a representative of the Organisation.

You must not comment as a representative of the Organisation unless you are authorised to do so.



Once authorised to comment, you must:

- disclose you are a worker of the Organisation, and use only your own identity or an approved official account;
- disclose and comment only on information classified as public domain information;
- ensure that all content published is accurate and not misleading, and complies with all relevant Organisation policies;
- ensure you are not the first to make an announcement (unless specifically given permission to do so);
- comment only within your authorised scope;
- ensure comments are respectful of the community in which you are interacting online; and
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws, and Organisation policies.



Once authorised to comment, you must not:

- post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, or is otherwise unlawful;
- use or disclose any confidential information; and
- make any comment or post any material that might otherwise cause damage to the Organisation's reputation (or that of its workers, members, customers, business partners and/or suppliers) or bring it into disrepute.

Personal use of social media

The Organisation recognises that a worker may use social media in their personal life.

This policy does not intend to discourage nor unduly limit your personal expression or online activities. However, you should be aware that the content you post and engage with in a personal capacity on social media may cause indirect or direct damage to the Organisation's reputation and interests where when you can be identified as a worker of the Organisation through your social media.

You should comply with this policy to avoid and minimise those risks. If you are unsure how to comply, you should seek guidance from the Organisation.



Where you can be identified as a worker of the Organisation, you must:

- only disclose and discuss publicly available information;
- ensure that all content published is accurate and not misleading and complies with all relevant Organisation policies;
- expressly state on all postings (identifying you as a worker of the Organisation) that the stated views are your own and are not those of the Organisation; and
- be polite and respectful to all people you interact with.



Where you can be identified as a worker of the Organisation, you must not:

- post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, or is otherwise unlawful;
- imply you are authorised to speak on behalf of the Organisation, or give the impression that any views you express are those of the Organisation;
- use your Organisation email address or any Organisation logos or insignia that may give the impression of the Organisation's official support or endorsement of your personal comment;
- assume the identity or likeness of another worker of the Organisation;
- use or disclose any confidential information or personal information obtained in your capacity as a worker of the Organisation;
- post images or videos of other workers or customers/ members without their permission; and
- make any comment or post any material that might otherwise cause damage to the Organisation's reputation (or that of its workers, residents, customers/members, business partners and/ or suppliers) or bring it into disrepute.

How can I report breaches of this policy?

The Organisation encourages all workers who become aware of conduct on social media that is in breach of this policy to report it immediately, in line with the below process.



1.

In the first instance, a worker seeking to make a report conduct that breaches this policy should contact a manager or supervisor that they trust.



2.

The manager or supervisor should ensure that they obtain the particulars of the complaint/allegations in writing, such as what occurred and when it occurred. Screenshots of the conduct should also be obtained.



3.

Where possible, and if appropriate in the circumstances, the Organisation will attempt to resolve the matter via a mediation process between the parties.



4.

However, if mediation is inappropriate or is unsuccessful, subject to the circumstances, the Organisation may arrange for an investigation.

The investigation will be conducted in accordance with the principles of natural justice.



5.

Depending on the nature and complexity of the complaint, the Organisation may engage an external investigator.



6.

Once the investigation is complete, the Organisation will make findings in relation to the conduct and confirm relevant findings and next steps with the affected parties in writing.

The Organisation will ensure that such reports are addressed in a timely and sensitive manner.

Confidentiality and Victimisation

Confidentiality

Reports and details of an investigation are subject to strict confidentiality and must only be disclosed to others on a need-to-know basis.

A worker who breaches confidentiality may face disciplinary action up to and including summary dismissal or cessation of engagement.

Victimisation

Victimisation is strictly prohibited and will not be tolerated by the Organisation.

Victimisation occurs where one worker subjects, or threatens to subject, another worker to any detriment because that worker has made a report, or is involved in an investigation conducted under this policy.

A worker who feels they are being victimised should report it in accordance with this policy.

A worker who victimises another worker may face disciplinary action up to and including summary dismissal or cessation of engagement.



What will happen if I breach this policy?

A breach of the obligations outlined in this policy may lead to:

- an employee being subject to disciplinary action up to and including summary dismissal; or
- termination of the engagement of any other worker, or cessation of their services being provided to the Organisation.

