The University of Queensland Union College
Social Media & ICT Policy

Statement of Commitment

We are committed to preventing and responding to gender-based violence, including technology-facilitated abuse, consistent with the National Plan to End Violence against Women and Children 2022–2032 and the Action Plan Addressing Gender-Based Violence in Higher Education.

Introduction

We provide you with access to information and communication technology (ICT) resources to support your study, work, communication and full participation in college life. This policy explains how to use Union College ICT resources safely, respectfully and lawfully, and how doing so supports our broader commitments under the Australian Universities Accord and the National Action Plan Addressing Gender-Based Violence in Higher Education.

We recognise that social media platforms such as Facebook, X (formerly Twitter), Instagram, TikTok, LinkedIn, Snapchat and many others are central to how you connect, share and participate in college life. Social media blurs the line between your personal and public life, and what you post can affect your safety, the safety of others and the reputation of Union College and the broader higher education sector. What you post on the internet is also permanent – this is called your digital footprint and it cannot ever be fully erased.

Purpose

Union College is your 'home away from home', but when you use our network, you are also using a UQ/UQ Commercial internet link. This means you must comply with the following:

- This policy
- The University of Queensland's ICT policies (including the Acceptable Use of UQ ICT Resources policy and Information and Communication Technology Policy)
- All relevant Commonwealth and state laws, including cybercrime, copyright, privacy, anti-discrimination and online safety legislation.

This policy also sets out the minimum standards for your use of social media while you live at Union College. It aims to:

- Help you use social media in ways that are safe, lawful and respectful
- Protect your privacy and the privacy and rights of others
- Prevent and address technology-facilitated abuse, including forms of gender-based violence, in line with the National Action Plan Addressing Gender Based Violence in Higher Education and the National Higher Education Code to Prevent and Respond to Gender Based Violence
- Support the Australian Universities Accord vision for safe, high-quality student experiences on campus and online.

Scope

This policy applies to:

- All residents using Union College ICT resources or the residential network
- Any device you connect to our network, whether owned by you or someone else
- Any use of our network to access the internet, whether for study, work or personal purposes.
- All residents using any social media platform, whether for personal use or, if authorised, on behalf of Union College
- Any content you create, share or engage with that identifies or could reasonably be linked to Union College, UQ or members of our community.

This policy applies to all IT resources used on our network.

Strategic context: safety, wellbeing and digital environments

We align this policy with:

- The Australian Universities Accord's emphasis on student welfare, safety and wellbeing, both on campus and online, and on high-quality digital learning environments
- The Action Plan Addressing Gender-Based Violence in Higher Education and the National Higher Education Code to Prevent and Respond to Gender-Based Violence, which treats technology-facilitated abuse (including image-based abuse, stalking, harassment and hate speech) as forms of gender-based violence and expects providers and accommodation services to prevent and respond to harm in digital as well as physical spaces.

We recognise that:

- Digital technologies are central to teaching, learning and community life, and are critical to the Accord's goals of access, participation and success
- The same technologies can be misused to perpetrate harassment, discrimination, bullying, hate speech, image-based abuse, and other behaviours that undermine safety, equity and inclusion.

This policy sets clear expectations so that our shared ICT resources support your learning and wellbeing without exposing you or others to avoidable harm.

Legal Compliance & Age Restrictions

You must comply with Australian law and the platform-specific terms and conditions when using social media. This includes:

- Online safety and age-restriction requirements under the Online Safety Amendment Act 2024 and related regulations

- Criminal and civil laws relating to harassment, stalking, threats, discrimination, image-based abuse, bullying, defamation, privacy, copyright and consumer protection.

In particular:

- You must not use social media to engage in unlawful behaviour, including threats, hate speech, serious harassment, incitement of violence, non-consensual sharing of intimate images, any form of or behaviour that may be considered bullying, or other forms of technology-facilitated abuse.

If your conduct may breach the law, we need to notify UQ, and may need to notify external authorities (such as eSafety or police) and cooperate with their investigations.

Your rights and responsibilities

Our commitments to you:

- We will provide you with access to the residential network and ICT resources that support your studies and participation in college life, subject to reasonable technical and security constraints.
- We will treat your use of ICT resources with respect for your privacy, while complying with the law and our obligations to safeguard the safety and rights of others.
- We will act on serious misuse of ICT resources, primarily conduct that may amount to discrimination, harassment, gender-based violence, threats or other unlawful behaviour, in line with our complaints, conduct and safety policies.

Your responsibilities:

- Use ICT resources in ways that are respectful, lawful and consistent with this policy, UQ policies and applicable laws.
- Avoid using ICT resources in ways that harm, harass, intimidate or discriminate against others, including through technology-facilitated abuse, image-based abuse or persistent unwanted contact.
- Protect your own and others' personal information online, and report any serious safety, harassment or illegal content concerns to an appropriate member of staff or via established reporting pathways.

Definitions

<u>What we mean by social media</u>

For this policy, "social media" includes, but is not limited to:

- Social networking platforms (for example, Facebook, X, LinkedIn, Bluesky, etc.)
- Video and photo sharing platforms (for example, Instagram, Snapchat, Pinterest, YouTube, TikTok, Threads, Discord, Vimeo, Flickr, etc.)

- Blogs and websites with comments or “your say” features, including personal, corporate and media-hosted blogs
- Public wikis and online collaborations (for example, Wikipedia, Reddit, etc.)
- Forums, discussion boards and groups, and online review sites (for example, Whirlpool, TripAdvisor, Yelp, Booking.com, etc.)
- Instant messaging services (for example, Facebook Messenger, WhatsApp, Snapchat, Viber, SMS, Telegram, Signal, etc.)
- Geo-spatial tagging and “check-in” features (for example, Foursquare and location tagging on other platforms etc.).

What we mean by ICT

ICT stands for Information and Communications Technology. This covers any device utilizing our Wi-Fi or Internet connections, Bluetooth on Campus including the use of printers.

Unacceptable use of ICT resources

To clarify expectations, we have provided examples of unacceptable use. These examples are not exhaustive.

You must not:

- Download, store, distribute or view offensive, obscene, indecent, pornographic, violent, racist, hateful or menacing material, including content that would reasonably be considered harassment, hate speech, gender-based violence (including image-based abuse and non-consensual sharing of intimate images - see Sexual Misconduct Prevention and Response Policy (RES0202)) or other serious harm
- Use ICT resources to bully, stalk, threaten, humiliate or otherwise harm others, whether they are residents, staff or people outside Union College
- Access or share sites that promote hate, extremist ideologies, or gratuitous violence
- Damage, tamper with, or destroy ICT equipment or systems belonging to Union College or UQ
- Use the network in ways that unreasonably degrade others' performance (for example, by downloading or uploading large volumes of non-study-related data or running applications that consume an unusually high share of bandwidth for extended periods)
- Download or stream copyright material from unlicensed sources or engage in any form of software piracy
- Use the network for illegal activities, including accessing or distributing illegal content, committing fraud, hacking, or other nefarious conduct

- Forge or misrepresent your identity or someone else's identity including via email, messaging, social media, or any other electronic communication. This is a serious breach and may also be a criminal offence
- Use University resources for unrelated business or to make a profit, in breach of UQ's policies on unrelated business activities.

Please be aware: law enforcement agencies, including the Australian Federal Police, have previously contacted us to request details of a resident alleged to have accessed unlawful content. While we do not routinely monitor individual access, we are legally obliged to provide log data and to cooperate if lawfully instructed to do so.

Network rules and technical requirements

To keep the residential network reliable and secure, you must follow these rules:

- Do not modify, tamper with or extend network services or wiring, including network jacks, cabling, hardware or cluster connections.
- Do not use the residential network to provide Union College or UQ network or internet access to anyone outside the Union College and University community. If access is necessary to directly support the University mission and is in compliance with UQ and Union College policies, you can offer an external party access to the Union College Visitors network. The information for this can be obtained at Reception.
- Remember that the residential network is a shared resource. You must not use applications or configure devices in ways that inhibit or interfere with others' use of the network, such as using an IP address not registered to you or running services that cause network outages.
- Do not connect routers, switches, or Wi-Fi extenders with DHCP or NAT enabled. These devices can breach network rules and cause widespread network failures if misconfigured and are therefore not permitted.

Failure to comply with these requirements may result in your residential network services being disconnected or restricted until any issues are resolved. Any costs we incur because of your actions may be passed on to you.

Privacy, personal information and online safety

To safeguard yourself and others, you agree that:

- You will not disclose sensitive personal information, such as your own or others' full names, addresses, bank account details, phone numbers, or other identifying information, in unsafe or inappropriate online contexts
- You will take reasonable care when using social media, messaging, and other online platforms to minimise the risk of identity theft, fraud, harassment, or other harm

- You will be alert for suspicious or harmful content, links and messages, and you will close or report them rather than engage with them.

We encourage you to report serious online safety issues—such as image-based abuse, persistent harassment, threats, or child exploitation content—through our internal reporting pathways and, where appropriate, to external bodies such as eSafety and the Queensland Police Service (QPS).

Technology-facilitated abuse and gender-based violence

Technology-facilitated abuse, including online harassment, image-based abuse, cyberstalking, and other forms of digital harm, is a form of gender-based violence. See our Gender-Based Violence Prevention and Response Policy (RES0201) and Sexual Misconduct Prevention and Response Policy (RES0202) for comprehensive frameworks.

Breaches involving serious misconduct will be investigated in accordance with the procedures outlined in our Addressing Concerns and Complaints Policy (RES0102).

You must not use ICT resources to:

- Target people because of their gender, sexuality, race, disability, religion or other attributes through harassment, threats or degrading content
- Share, create, or manipulate intimate images of others without their consent (image-based abuse)
- Engage in stalking, doxxing (sharing private information), or persistent unwanted contact that causes fear or distress.

You must not use social media to:

- Bully, harass, threaten, vilify, ridicule or humiliate others
- Engage in or facilitate image-based abuse, including creating, sharing or threatening to share intimate images or recordings without consent
- Stalk, dox (share private information), or engage in persistent unwanted contact that causes fear, distress or harm
- Promote or normalise gender-based violence, including sexual assault, sexual harassment or coercive control.

If we receive a disclosure or report of social media behaviour that may amount to gender-based violence or other serious harm, we will:

- Prioritise the safety, wellbeing and wishes of the person affected, using trauma-informed practice
- Manage the matter through our Addressing Concerns and Complaints Policy and other relevant policies (such as our Sexual Misconduct Prevention and Response and Gender-Based Violence

Prevention and Response policies, as well as our Child and Young Person Protection Policy if applicable) with procedural fairness for all involved

- Cooperate with UQ, regulators and law enforcement where required.

Privacy, Consent, & Filming in Residential Spaces

Living in a residential community means you share spaces with others who have a right to privacy and to feel safe.

You must:

- Respect other people's privacy. Do not tag them, post photos or videos of them, share their content or reveal their location without their permission.
- Obtain consent from all visible individuals before posting videos filmed in residential areas, corridors, bathrooms, common rooms or other shared spaces.
- Avoid posting content that reveals sensitive personal information about yourself or others (such as home addresses, phone numbers, bank details, health information or student IDs) particularly in ways that could expose anyone to harm.

We encourage you to:

- Use privacy and security settings on your accounts
- Avoid saving passwords on shared devices
- Think carefully before sharing content that could be misused if taken out of context.

AI, Deep-Fakes, & Content Creation

Emerging technologies, including genAI, can be helpful tools but also create new risks for misinformation, manipulation and harm.

If you use AI tools for social media content creation, you must:

- Disclose, where appropriate, that AI has assisted in creating your content (for example, "Created with AI assistance")
- Check the factual accuracy of AI-generated content before sharing it, especially where it relates to Union College, UQ, public health, safety or other sensitive topics
- Not upload confidential or sensitive College-related data (including internal documents, student details or incident information) to third-party AI platforms
- Not create, share or amplify deep-fake or manipulated media that could deceive, defame or harm others.

We encourage you to use tools such as reverse image search or verification services when you are unsure whether images or videos are genuine, and to seek advice from staff if you come across suspicious or harmful content.

Prohibited & Restricted Content & Activities

You must not use social media in ways that:

- Bring Union College or UQ into disrepute
- Share false, misleading or malicious comments about the College, staff, residents or partners
- Disclose confidential information or intellectual property belonging to Union College, UQ or others, such as internal documents, non-public decisions, private communications or commercially sensitive information
- Promote third-party products or services using College branding, logos, uniforms or locations without written authorisation ("social commerce")
- Use College branding or claim to speak on behalf of Union College without prior approval from the Deputy Head of College – Student Life.

If you are authorised to post on behalf of Union College:

- You must follow any additional guidelines and approval processes provided to you
- Your content should align with our values, policies and legal obligations, and must be accurate, respectful and in line with brand and style expectations.

Responding To Harmful or Inappropriate Social Media Behaviour

If you experience or witness harmful behaviour on social media (such as harassment, threats, hate speech, gender-based violence, impersonation, or misinformation), we encourage you to:

- Clearly ask for the behaviour to stop, if it is safe to do so
- Stop engaging with the person if the behaviour continues
- Keep evidence, such as saving texts, messages or emails and taking screenshots of posts or comments
- Block unwanted accounts or mute conversations where appropriate
- Report the behaviour to the platform and, if relevant, to eSafety or other bodies
- Report the issue to the Resident Wellbeing Lead or Deputy Head of College, especially where the behaviour involves residents, staff or Union College, so we can support you and consider further action.

We will listen, support you and, where appropriate, act in line with our complaints and safety policies and our national obligations around gender-based violence and student wellbeing.

Misinformation, Disinformation, & 'Fake News'

Social media can quickly spread false or misleading information. To help protect yourself and others, you should:

- Be skeptical of sensational or "clickbait" headlines, especially those in all caps with excessive punctuation
- Check the URL and website – fake sites often mimic real news outlets with minor changes in the address
- Investigate the source – look for credible, reputable organisations and authors with a track record of accuracy
- Cross-check information with trusted and independent sources before sharing
- If you are unsure whether something is true, do not share it.

This supports the Accord's emphasis on critical thinking, digital literacy and responsible engagement with information in higher education.

Scams

Scams are increasingly online endeavours. We expect all residents to be diligent and careful in interactions online to protect themselves and others in the community, as well as our College network.

Scams are dishonest schemes to gain money or possessions from someone fraudulently. They can occur quickly, through one interaction, or over a prolonged period of time. Scams are illegal in Australia under Federal and State Legislations. They can take the form of:

- Romantic scams
- Blackmail
- Giveaway scams
- Gaming scams
- Scholarship scams
- Government scams

If you are a victim of a scam, or think you might be, you should immediately book in to see the Resident Wellbeing Lead. The Resident Wellbeing Lead will not judge you, but will ask questions to get all the information to ensure we support you in taking the appropriate next steps.

A report of this behaviour by a Union College resident will be subject to our Addressing Concerns and Complaints Policy and will be referral to the Queensland Police Service. We will comply with and support their investigation/s.

Extremist recruitment

Extremists (a person or group who hold/s extreme political or religious views, especially one who advocates illegal, violent, or other extreme action) often target young adults in a university setting. They will appeal to targets through a foot-in-the-door technique, where they will offer a logical or sympathetic argument for their cause, then use initial agreement as leverage to radicalize their target. This predatory behaviour is becoming increasingly common online.

Illegal, violent or other extreme actions (including bullying and intimidation, manipulation and abuse) go against Union College values. A report of this behaviour by a Union College resident will be subject to our Addressing Concerns and Complaints Policy.

If you suspect you may be being initiated into an extremist group, are part of an extremist group and would like not to be, or you witness concerning behaviour (online or in person), please book in to see the Resident Wellbeing Lead immediately. The Resident Wellbeing Lead will not judge you, and is here to offer support for you in navigating this environment.

Consequences for breaches

If you breach this policy, consequences may include:

- Restriction of your access to ICT resources
- Disconnection from the residential network until problems are resolved or a third party resolves technical issues
- Behavioural or disciplinary action under the Resident Code of Conduct (RES0101) and Addressing Concerns and Complaints Policy (RES0102)
- Referral to UQ for breaches of UQ ICT policies
- Referral to external authorities (such as police or regulators) where your conduct may be unlawful or poses a serious risk to others.

We will apply consequences in a fair, proportionate and transparent manner, consistent with our broader obligations under the Universities Accord, the National Student Charter and the forthcoming National Student Ombudsman arrangements.

Resident agreement

As a condition of residence and network access, you agree that:

- You will refrain from accessing or engaging with online spaces that would reasonably be considered offensive due to pornographic, racist, hateful, violent, illegal or otherwise harmful content
- You are responsible for monitoring and appropriately rejecting materials, links, dialogue and information you encounter or receive online
- You will not damage computer systems or networks

- You will not misuse your own or others' personal information
- You understand that if you breach this policy, you may have your access to the network restricted or denied, and you may face further disciplinary action.

Review and continuous improvement

We will review this policy at least annually, and sooner if:

- UQ updates its ICT policies
- Relevant laws or regulations change
- New expectations arise from the Australian Universities Accord, the National Student Charter, the National Higher Education Code to Prevent and Respond to Gender-Based Violence or related reforms
- We identify issues in practice or through feedback that require updates.

Document Number: POL003
Topic: Use of Union College ICT resources, Resident Agreement
Approval Authority: Head of College & CEO
Last Approval Date: January 2026
Review Date: December 2027 (or earlier if legislation or UQ policy changes)
Audience: Current and future residents, parents and carers, Union College workers and Board, key stakeholders and regulators

DISCLAIMER: Union College's policies and procedures for the prevention of and response to gender-based violence, including sexual misconduct, are designed to be consistent with and aligned with The University of Queensland's Sexual Misconduct Prevention and Response Policy and associated procedures, as well as UQ's broader frameworks and commitments relating to gender equality, respect, and safe, inclusive campus communities.