

The University of Queensland Union College Resident Acceptable Use of IT Resources Policy

Purpose and scope

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.

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 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.

This policy applies to all IT resources used on our network. Social media platforms are addressed in our Acceptable Use of Social Media Policy (RES0402), which provides further detail on social media conduct and complements this policy. Both policies apply to the use of IT resources.

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 forthcoming 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.

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.

Unacceptable use of ICT resources

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

You must not knowingly:

- 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 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 University community, except when it directly supports the academic mission and complies with UQ policies.
- 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.

If we receive a disclosure or report that you have used ICT resources in ways that may constitute gender-based violence or serious harassment, we will:

- Prioritise safety and support for the person affected, in a trauma-informed way
- Manage the matter through our Addressing Concerns and Complaints Policy and other relevant policies, ensuring procedural fairness for everyone involved
- Cooperate with UQ, regulators and law enforcement where required.

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: RES0401

Topic: Use of Union College ICT resources, Resident Agreement

Approval Authority: Head of College

Last Approval Date: January 2026

Review Date: December 2026 (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.