



A quick guide to the *Acceptable Use of ICT Resources Policy*



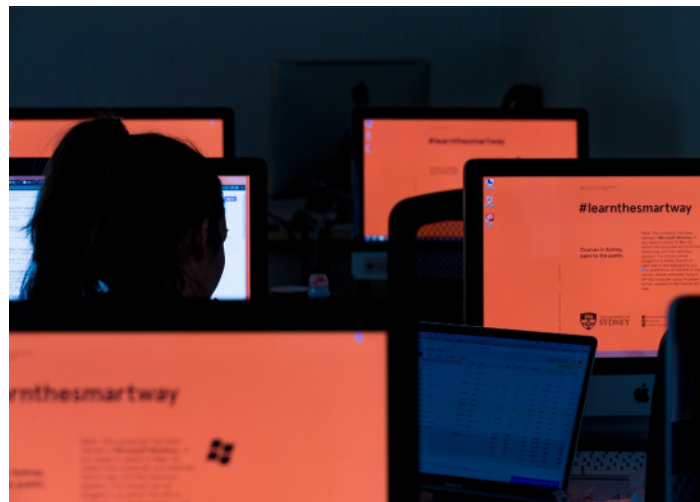
*This is a **general guide** only. You can find the full policy in the Policy Register.*

Summary

This policy prescribes how the University's Information and Communications Technology (ICT) resources may be used.

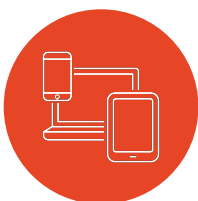
It explains what uses are acceptable and what are unacceptable, and assigns responsibilities to ensure that our resources are used **legally, ethically and responsibly**.

It applies to anyone who uses our ICT resources: staff, affiliates, students, contractors and visitors.



What are the University's ICT resources?

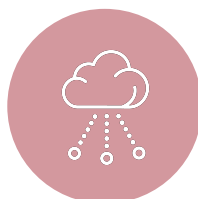
This term includes any and all aspects of University-provided information and communications technology, and the digital information it handles. This includes:



Hardware or devices



Business or technology solutions such as applications, software as a service, telecommunications systems, media services, file and print services and email services



Software, cloud based services, data centres, or networks



Information stored, processed or transmitted within an ICT service or asset

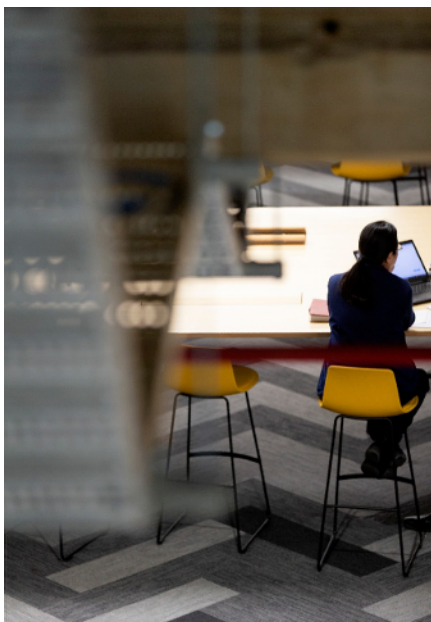
What is acceptable use?

Acceptable use:

- Complies with applicable laws, University policies and the **Cyber Security Technical Standards**
- Is consistent with **our values**
- Is consistent with the University's commitment to freedom of speech and academic freedom
- Includes reasonable steps to protect the University's resources and information from theft, misuse, damage or unauthorised access
- Includes limited personal use, provided it is lawful and does not adversely affect the University's operations
- Includes using personal devices to connect to, or remotely access University ICT resources, provided you comply with the security standards
- Includes connecting personal disability assistive devices where necessary



What is unacceptable use?



You must not use University ICT resources to:

- Bully, harass, sexually harass or intimidate anyone
- Unlawfully discriminate against anyone
- Access, store or transmit prohibited or restricted material without permission
- Breach privacy or intellectual property requirements
- Gain unauthorised access to external services
- Damage or corrupt the University's data, software or hardware
- Damage or corrupt anyone else's data, software or hardware
- Send junk mail, chain mail or for-profit messages
- Make excessive use of University resources

The policy provides further detail about what is prohibited and restricted material, and how to obtain necessary permissions.

User responsibilities

You are responsible for all activity from your University accounts. If you identify or suspect a cyber security event or vulnerability you must contact the Shared Service Centre or ICT Cyber Security Operations Team as soon as possible.

You must not:

- Lease, loan or make any University ICT resources available to a third party
- Use University ICT resources for unauthorised financial or commercial purposes
- Use University ICT resources to generate or process cryptocurrency without permission



Terms of Use



University ICT resources are not guaranteed to be available or defect-free



Use of University ICT resources is not private and may be monitored and recorded as permitted by law



The University may limit your use of its ICT resources and inspect the resources and the data held by them



The University may require you to complete specified training



What is a breach of this policy and what happens?

You breach the policy if you:



Act inconsistently with it



Help or encourage someone else to act inconsistently with it



Promote conduct that breaches the policy on social media or in some other way

If you breach the policy:

- We may limit or cut off your access to University ICT resources
- You may be subject to misconduct proceedings
- You may breach other University policies, such as codes of conduct or policies against bullying, harassment or discrimination
- You may breach laws, and be subject to civil or criminal proceedings

