Staying Safe Online

Think before you click: Always exercise caution and remember that attachments in unexpected email messages or from unknown senders will often contain malicious content designed to infect your computer. Fraudulent web addresses will lure you into providing your login details to gain personal information that can be used against you.

Learn to recognise phishing attempts: A phishing email is a fraudulent email used to solicit personal information such as your password or banking details. Phishing emails often try to create a sense of urgency by stating such things as "A recent security upgrade means that you have to log on to be protected".

Tips to help you recognise a phishing email:

- You are being asked to send personal information;
- The sender address look suspicious;
- The email provides no contact details;
- The offer seems too good to be true;
- The message contains poor spelling and grammar;
- A sense of urgency, such as "urgent action required!"
- When you hover over the link it looks suspicious.

If you have received a phishing email or clicked on a malicious website, contact University IT immediately.

For more information on how to stay secure online please visit the UWA Cyber Security website:
cybersecurity.it.uwa.edu.au

THE UNIVERSITY OF WESTERN AUSTRALIA

Information Technology

The University of Western Australia
M463, Perth WA 6009 Australia
Tel: +61 8 6488 1515
Email: servicedesk@uwa.edu.au

CRICOS Provider Code: 00126G

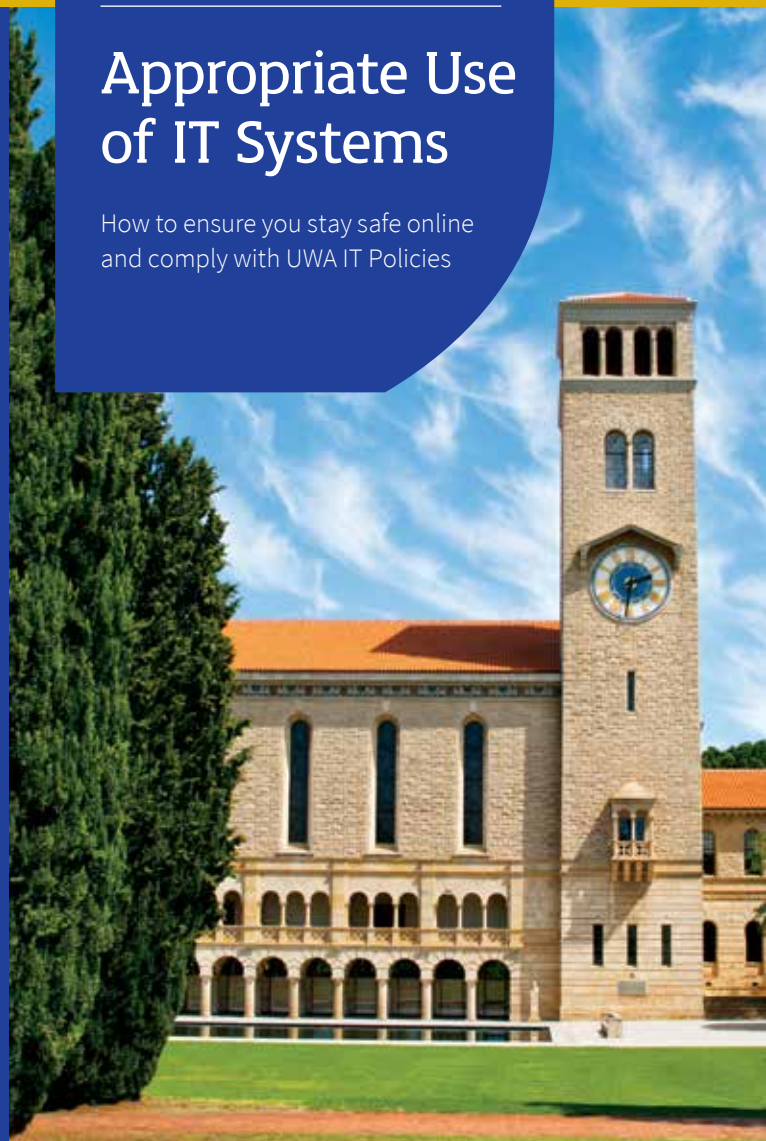
DCS000071

THE UNIVERSITY OF WESTERN AUSTRALIA

Information Technology

Appropriate Use of IT Systems

How to ensure you stay safe online and comply with UWA IT Policies



IT at UWA

The University's Information Technology resources provide a rich array of services to the UWA Community. Ensuring the continuity and availability of these resources is the responsibility of both the University IT Team and University IT Users. Users are defined as staff, students, authorised visitors and anyone connecting personally owned devices such as laptops, smart phones and tablets to the University network.

IT services provided by the University are intended to be used in a manner that is consistent with the University's mission.

University IT is committed to:

- Providing users with secure and timely access to IT resources necessary to undertake their research, work or study; and
- Maintaining a reliable IT infrastructure to support the University's operations.

UWA IT Policies

As a condition of the use of IT, users are required to comply with the University's Computer and Software Use Regulations which can be found within the online University Policy Directory **www.governance.uwa.edu.au/university-policy-management-framework**

The Appropriate Use Guidelines on the next page are intended to provide a framework for the protection and effective utilisation of UWA IT resources.

Appropriate Use of IT Systems

Security is everyone's responsibility. By following the below Appropriate Use Guidelines we are all working together to ensure our University is not exposed to risks including the loss of confidentiality, integrity or availability of our data and systems. Please consult the full University Computer and Software Use Regulations if there is any doubt as to what is expected of you.

You should not

- Share your University username and password with others or use someone else's username and password.
- Access, copy, alter or destroy any University data, emails or other systems that you are not specifically authorised for.
- Possess, download, upload or distribute any material that may be illegal or subject to copyright, including pirated films and other unlicensed, unlawfully obtained or unauthorised media or software, as well as any malicious software or offensive material.
- Access, distribute or share University course materials, software licenses or research materials without appropriate authorisation.
- Use University IT systems and services to distribute any unsolicited emails such as SPAM or malware.
- Use IT systems and services to bully, stalk or harass anyone.
- Use IT resources to run a business or e-commerce platform.
- Use your University staff or student emails for registration of personal social media or any other personal accounts.

You should

- Only use University IT systems and services for which you are specifically authorised to use.
- Use University IT systems and services for appropriate and authorised purposes only i.e teaching, learning, research and academic purposes.
- Report any suspicious behaviour or violations of the University's Computer and Software Use Regulations to University IT.
- At all times lock your computers and mobile devices when you are leaving them unattended for any length of time.
- Avoid using the same password for your University and personal accounts.
- At all times comply with all relevant University policies and only use University IT systems and services in a way that is ethical and lawful, while respecting the privacy and personal rights of others.

Cyber Security Support

We are here to help.

Please contact us for any of the following:

- To report an IT security incident;
- If you have any security questions or concerns;
- If you need advice on securing your systems; or
- If you have a case for an exemption to the University's Computer and Software Use Regulations, based on teaching, learning and/or research requirements.

Contact your local SDC IT Team

cybersecurity.it.uwa.edu.au

servicedesk@uwa.edu.au

(Subject: attention to the cyber security team)

ABLE:	ext 1523 (08 6188 1523)
EMS:	ext 1999 (08 6488 1999)
Science:	ext 2999 (08 6488 2999)
Central:	ext 1515 (08 6488 1515)
HMS:	08 6457 7325 (external)