IT Acceptable Use Policy – SUMMARY

1. This document is a summary of the key points in the University's Acceptable Use Policy (AUP). Staff, Faculty and students are advised to read the full policy document, which is published on the University website.

2. You must:

   2.1 Change your password and inform the IT Department immediately if you suspect a third party has access to your account or to University's data and/or systems.

3. You must NOT:

   3.1 Use someone else's username and password to access University IT systems;

   3.2 Attempt to access data that you are not authorised to use or access;

   3.3 Give or transfer University data or software to any person or organisation outside the University without the authority of the University;

   3.4 Use profanity, obscenities, or derogatory remarks in communications;

   3.5 Access, download, send or receive any data (including images), which the University considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material;

   3.6 Use University networks or social media to engage in any act of bullying, harassment or hatred, whether directed towards other students, staff or externally;

   3.7 Use the University's internet or email to gamble, make personal gains or conduct a personal business;

   3.8 Use University systems in a way that could affect their reliability or effectiveness;

   3.9 Publish any internal or confidential information externally;

   3.10 Send unprotected sensitive or confidential information externally;

   3.11 Download any software, music recordings or other materials that you know to be fakes or "pirate copies";

   3.12 Use any unlicensed or unauthorised software on University computers;

   3.13 Remove or disable anti-virus software from University devices;

   3.14 Attempt to remove any virus, malware or suspected infection without consultation with the IT Department;

   3.15 Distribute a virus or other harmful code;

3.16 Perform any unauthorised changes to University IT systems or information;

3.17 Connect any unauthorised device to the University network;

3.18 Engage in any acts of hacking, including attempting to access another user's account or any form of sabotage, for example causing a denial of service (DoS) attack;

3.19 Generate adverse publicity or tarnish the University's name;

3.20 Disclose confidential information about the University;

3.21 Any other activity which could bring the University into disrepute.

VERSION MANAGEMENT

Responsible Department: IT			
Approving Body: University Board (on recommendation of Operations Committee)			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1.0	Initial Version	24 July 2025	September 2025
1.1	No changes to the policy; reviewed and approved by University Board for AY 2026–27.	5 May 2026	September 2026
	Restricted Access? *Tick as appropriate*: Yes ☐ No X		