ACCEPTABLE USE OF IT RESOURCES – MISUSE SCHEDULE

SECTION 1 – PURPOSE

(1) The purpose of this schedule is to define misuse in relation to the Acceptable Use IT Resources Policy.

SECTION 2 – SCHEDULE

(2) 'Misuse' includes, but is not limited to:

(a) use for any purpose other than an authorised purpose;
(b) use that causes or contributes to a breach of any provision of a law, statute, regulation, subordinate instrument or code of practice or conduct applying to the University or to which users are subject;
(c) use that contravenes a University statute, regulation, rule, policy or procedure;
(d) creating, transmitting, storing, downloading or possessing illegal material;
(e) accessing, displaying, copying, downloading, distributing, storing or sharing pirated software, games, video, music, images, fonts, or other copyright material;
(f) the deliberate or reckless creation, transmission, storage, downloading, or display of any offensive or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the appropriate use of Information Technology Resources for properly supervised University work or study purposes;
(g) use which constitutes an infringement of any intellectual property rights, or copyright of another person or organisation;
(h) communications which would be actionable under the law of defamation;
(i) communications which misrepresent a personal view as the view of the University;
(j) use which constitutes unauthorised recording, publishing, or communication of University lectures, tutorials, meetings or conversations;
(k) deliberate or reckless undertaking of activities resulting in any of the following:
    a. the imposition of an unreasonable burden on the University's Information Technology Resources;
    b. corruption of or disruption to data on the University's Information Technology Resources, or to the data of another person or organisation;
    c. disruption to other Authorised Users; or
    d. introduction or transmission of any hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs in any form including hyperlinks, executable code, scripts, active content, and other software into the University's Information Technology Resources.
(l) circumventing authentication or access control measures, security or restrictions upon the use of any Information Technology Resources or account, including the unauthorised distribution or use of tools for compromising security, including but not limited to password guessing programs, cracking tools, packet sniffers or network probing tools;
(m) spread betting online without prior written approval from the Chief Information Officer. Permission can only be granted for the purposes of research and in consultation with the relevant Head of Department or Executive Dean.
(n) gambling, other than participation in approved football-tipping and like competitions

where the primary purpose is social rather than financial;

(o) accessing pornography without prior written approval from the Chief Information Officer. Permission can only be granted for the purposes of research and in consultation with the relevant Head of Department or Executive Dean.

(p) use of any Information Technology Resources for sending junk mail or unsolicited bulk messages without University approval, for-profit messages, or chain, hoax or scam letters or messages;

(q) use of any Information Technology Resources for the purposes of any private business whether for profit or not, or for any business purpose other than University business, without prior approval from the Chief Information Officer or the Vice-Chancellor;

(r) subscribing to list servers, mailing lists and other like services for purposes other than University work or study or limited personal use;

(s) participation in online conferences, chat rooms, discussion groups or other like services for purposes other than University work or study or limited personal use;

(t) unauthorised accessing of information, including but not limited to unauthorised access to servers, hard drives, email accounts or files;

(u) unauthorised reserving of, or exclusion of others from using, any Information Technology Resources;

(v) breaching the University's Privacy Policy;

(w) performing an act which will interfere with the normal operation of any Information Technology Resources;

(x) unauthorised use of the University logo;

(y) representing that a message or material comes from another person without that person's authorisation;

(z) knowingly running, installing or distributing on any Information Technology Resources a program intended to damage or to place excessive load on any Information Technology Resources, including without limitation programs in the nature of computer viruses, Trojan horses and worms;

(aa) failure to comply with the conditions of use imposed by an external provider when that provider's equipment or services are used in conjunction with any Information Technology Resources;

(bb) providing a password or other means of authentication for any Information Technology Resources to another person without prior written approval from the Chief Information Officer, or failing to take reasonable care to protect a password or other means of authentication for any Information Technology Resources from being accessed or used by another person;

(cc) failing to exercise reasonable care in the use, management and maintenance of Information Technology Resources, including but not limited to taking reasonable steps to ensure security and integrity of Information Technology Resources, including protection of equipment, systems and data from theft, unauthorised use or viruses;

(dd) failing to comply with any reasonable instruction given by or with the authority of the University copyright officer to remove or disable access to material;

(ee) using computing processing resources owned or operated by the University or computer resources powered by electricity provided by the University to perform mining of cryptocurrencies or brute forcing of cryptographic hash values for personal gain;

(ff) aiding, abetting, counselling or procuring a person to do any of the things referred to in paragraphs (a) to cc);

(gg) inducing or attempting to induce a person to do any of the things referred to in paragraphs (a) to (cc);

(hh) being in any way, directly or indirectly, knowingly concerned in, or a party to, any of the things referred to in paragraphs (a) to (cc);

(ii) conspiring with others to do any of the things referred to in paragraphs (a) to (cc); and

(jj) attempting to do any of the things referred to in paragraphs (a) to (cc).

SECTION 3 – NOTES

Status and Details

Status	Current
Effective Date	28 April 2021
Review Date	April 2024
Approval Authority	Vice-President, People and Services
Approval Date	28 April 2021
Expiry Date	Not Applicable
Responsible Executive	Nicole Gower Vice-President, People and Services
Responsible Officer	Tim Hume Chief Information Officer +61 2 9850 1660
Enquiries Contact	Jeremy Koster Chief Information Security Officer +61 2 9850 1987