ACCEPTABLE USE OF TECHNOLOGY POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	N/A
Next Review	January 2024
Approval	SLT 21/01/05
Effective Date	January 2021

Purpose:

Massey University provides many business tools to its staff to enhance their productivity and jobs. We require these systems to be used in a responsible way, ethically, and in compliance with all legislation and Massey University policies. Non-compliance could have a severe, negative impact on the University and its employees and clients.

Key success factors:

Staff understand how to use technology responsibly so that University information and people are protected.

Audience:

All users or anyone using technologies or systems to access, transfer or store University information. Users include University staff or anyone performing work on behalf of the University (including contractors, consultants and volunteers).

Policy:

All use of technology to store or transfer University information or conduct University business complies with our policy on Staff Conduct and all relevant laws, regulations, policies and standards. Staff are required to take particular care when handling student or classified information to keep it safe from unauthorised access, loss, or misuse, and includes any technology on which it is held or transferred. To meet the University's policy on Staff Conduct, users:

- must keep personal use of University technology (including emails or internet use) within reasonable limits, making sure it does not interfere with your work or University business
- must never use University information or technology for anything illegal or which may bring Massey University into disrepute; including infringement of copyright, or harassing or sharing offensive material with co-workers, our partners, or our students
- must be mindful of the effect on University (and personal) reputation in relation to any use of social media whether personal or work-related. Social media leaves a permanent record and electronic footprint. Using social media in such a way as could bring the University into disrepute will be actionable as a disciplinary matter.
- right of access to University technology to store or transfer Massey information (including email) ceases with the termination of employment.

Roles and responsibilities:

The Information Technology Services department is responsible for:

- proactively monitoring the use of technology to keep information and people safe and manage any impact on University reputation or functions. Where necessary this will include:
    - monitoring private and personal use of both Massey University-owned hardware and networks
    - the removal of information where it is offensive or illegal or impacts University business
    - the removal of University-owned equipment as part of disciplinary or criminal investigations.

Staff are responsible for:

- only using devices/software provided for you by the University. If you choose to use other software/devices not sanctioned by the University, you are personally responsible for ensuring the security and licensing of these items and ensuring that the loss or misuse of University information does not occur as a result
- protecting technology and information from loss and misuse by following Massey University policies and guidelines for use and protection of:
    - University passwords and smartcards, as they protect access to our information. See Massey University Information Security Manual for guidelines on how to select a secure password
    - any device used to handle University information; including laptops, desktops, tablets mobiles, and any form of mobile storage device. Ensure devices have up to date and patched operating systems and active anti-virus protection. See Devices definition, this policy
- reporting the loss or breach of University-owned technology as soon as you become aware of it to Massey University Service Desk and your Manager
- only sharing University or student information where it is explicitly authorised and required, and ensure that you have followed the required information sharing procedure for the information being handled
- keeping University information safe by using the Massey provided email account for undertaking University work. Personal email accounts must not be used for conducting University business. Some exceptions do apply for instance, a personal email account used during the recruitment process
- only installing software or technology on University devices where sanctioned and following related processes. Work-related applications may be downloaded on to University mobile devices from official or approved application stores
- keeping safe from malicious attacks (such as suspicious phishing emails, texts or website links) and quickly seeking advice from the Massey University Service Desk for any suspected information loss. (For example, if you have been tricked into sharing your password or sent University information to an incorrect recipient). See the Information Security Manual for guidelines on how to best protect your information.

Definitions:

Classified Information consists of confidential information which has been classified using the University's Information Security Classification Framework.

- IN CONFIDENCE information consists of information which if compromised would be likely to impede the effective operation of Massey University or adversely affect the privacy of its students or staff

- SENSITIVE information consists of information which if compromised would be likely to seriously damage the reputation of Massey University or endanger the safety of its students or staff.

Devices include, but are not limited to laptop computers and netbooks, tablet devices, smartphones, portable storage such as removable hard drives, USB memory sticks and data cards, portable audio visual equipment including data projectors, cameras etc.

Personally owned devices means any device that is held personally by an individual in a private capacity.

University issued device means any device that has been purchased, is owned or leased by the University (regardless of the source of funding).

University information means information relating to or connected with the University's business or affairs.

Relevant legislation:

Copyright Act 1994
Films, Videos, and Publications Classification Act 1993
Harmful Digital Communications Act 2015
Human Rights Act 1993
Privacy Act 1993

Legal compliance:

Copyright Act 1994
Email and the Internet make it very easy to copy the work of others. However, the Copyright Act 1994 makes it illegal to make or distribute copyright material without specific authorisation from the copyright owner. The University absolutely forbids the use of its computer and network facilities for a purpose which constitutes an infringement of copyright.

- No material is to be used without the written permission of the copyright owner.
- Copyright information is provided at the following intranet address: http://copyright.massey.ac.nz/

Note that the legal ownership of messages may not reside with the originator. For example, the ownership of intellectual property in the messages may rest with the University or other parties, depending on contracts, statutes and policies outside this document.

Films, Videos, and Publications Classification Act 1993
This Act classifies (i.e. censors) publications. It is illegal to possess, own, sell, hire, give or buy an objectionable publication. Therefore, users should not intentionally access, send or download objectionable material by Email or through the Internet.

Section 3 of the act states that material is "objectionable" if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good".

Harmful Digital Communications Act 2015
This Act aims to deter, prevent and lessen harmful digital communications. Harmful digital communications include cyber bullying and harassment, eg: sending or publishing threatening or offensive material or spreading damaging rumours.

Human Rights Act 1993
The Human Rights Act 1993 prohibits Massey University from discriminating against any employee or contractor on the grounds of sex, marital status, colour, race, ethnic or national origin, religious belief, disability, age, political opinion, employment status, family status or sexual orientation. It is unlawful to discriminate or to treat people unequally or less favourably on the grounds set out in the Act.

Privacy Act 1993
Email communications and web activity may be monitored from time to time to support operational, maintenance, auditing, security and investigative activities. The Privacy Act 1993 governs the collection and use of information held by the University for the purposes of its management and administration. Personal information held for these purposes must not be used for other purposes. Release of personal information otherwise than in accordance with the terms of the Privacy Act is strictly prohibited.

Related procedures / documents:

Information Security Classification Policy
Information & Technology Security Policy
Massey University Collective and Individual Employment Agreements
Massey University Information Security Manual
Policy on Staff Conduct
Electronic Password Policy
Student Academic Integrity Policy
Intellectual Property Policy
Desktop Hardware and Software Policy

Document Management Control:

Prepared by: Chief Information Officer
Authorised by: Deputy Vice-Chancellor, Finance and Technology
Approved by: SLT 21/01/05
Date issued: November 2019
Next review: January 2024