Acceptable Use of IT Systems Policy

Contents

Our Values

LTSA values a safe, inclusive, respectful workplace with a focus on providing our team members with an environment that supports their health, wellbeing, productivity, and effectiveness.

This policy aims to outline LTSA expectations of team members using LTSA and La Trobe University's (LTU) ICT systems, network and facilities.

Policy Application

This policy does not form part of any contract of employment or any industrial instrument. It will be subject to regular review and may be amended by LTSA from time to time.

This policy applies to the following persons, collectively referred to in this policy as 'team members':

a) prospective and current full-time, part-time and casual employees;

b) Governing Board of Director’s;

c) volunteers;

d) agents and contractors engaged from time to time;

e) elected student representatives; and

f) any other users of LTSA and LTU’s ICT facilities.

This policy applies:

a) at the workplace and when team members are working for LTSA away from the workplace, including the home;

b) to use of LTSA and LTU’s ICT systems and devices outside of working hours; and

c) to personal equipment (e.g. mobile phones and personal devices) that are used to access LTSA and LTU’s systems or emails

Definitions

“Confidential Information”

Includes but is not limited to: confidential company business of LTSA; non-public information about LTSA and affairs of LTSA such as: pricing information, internal cost and pricing rates, production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; honoraria payments; arrangements and dealings with LTU; contractual arrangements with third parties; tender policies and arrangements; all financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from LTSA or obtained in the course of working or providing LTSA services that is by its very nature confidential.

“Computer”

Includes all laptop computers, tablets and desk top computers.

"LTSA/LTU Network"

Means all software, hardware, computer networks and other technology which LTSA provides or makes available for use by team members for the business purposes of LTSA. This includes, but is not limited to:

a) telephone systems and hardware (including hand-held devices and facsimile devices when connected to LTSA's communication systems);

b) internet and electronic mail access, including those issued to Clubs & Societies, and LTU issued LTSA business email accounts and hardware; software and networks to facilitate website access; LTSA website and all modules within; electronic mail delivery and storage; Outlook Zoom and Microsoft Teams; teleconferencing or other electronic communication or dissemination of information;

c) LTSA's surveillance and security systems (including those systems facilitating physical access to the offices of LTSA across all campuses);

d) all document systems and tools facilitating document creation, management and access;

e) all printers, photocopiers and similar equipment; and

f) all data (including without limitation Confidential Information and Personal Information) in the above.

“Mobile Device”

Includes all such mobile devices which are used by team members. Such devices include, but are not limited to, mobile phones, smart phones, notebooks, digital cameras, hand-held devices, USB memory sticks and other storage devices, and other electronic devices used to access social networking sites or a social media platform.

“Intellectual Property”

Means all forms of intellectual property rights throughout the world including copyright, patent, design, trademark, trade name, and all Confidential Information and including know-how and trade secrets.

“Personal Information"

Means all information and opinions, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion. Examples include a person's name, address, telephone number, date of birth or photograph and may be contained in a resume or personnel file.

“Use of IT systems and devices”

Includes, but is not limited to, the following:

a) email;

b) instant messaging (SMS);

c) voicemail;

d) blogs/micro-blogging;

e) social and professional networking sites;

f) video and photo sharing websites;

g) document sharing websites;

h) forums and discussion boards;

i) wikis and online collaboration;

j) viewing material electronically;

k) browsing and publishing on the LTU intranet and internet;

l) downloading or accessing materials from the internet or other electronic devices;

m) file transfer, storage and sharing;

n) web and video conferencing;

o) podcasting and vodcasting;

p) streaming media;

q) online discussion groups and chat facilities;

r) subscriptions to list servers, mailing lists, websites or other like services; and

s) copying, printing, saving or distributing of electronic material

Access to the LTSA/LTU Network

Only team members that have been provided with a username and password by LTU’s IT Service Provider may access the LTSA and LTU Network. No users may provide access to LTSA or LTU’s Network, including by providing their username and password, to any other person for any reason, other than with the Governance and Operations Officer’s (GOO) prior approval.

A username and password will only be provided on completion of appropriate training as determined by the GOO or in their absence, the 2IC/Campus Coordinator.

Team members:

a) may only access those parts of the LTSA and LTU Network that are reasonably necessary to perform their duties;

b) must not access any part of the LTSA and LTU Network, including any document stored on the Network, which is not related to their duties and which a reasonable person in the circumstances would understand contained information that was not intended to be viewed by an individual in their position. Should a team member inadvertently access such information, they must immediately exit it and notify the GOO.

c) should not assume that, because they may technically be able to access a given part of the Network, they are authorised to do so. If team members are unsure about whether they may access any information on the Network, they should contact the GOO prior to accessing.

From time to time, team members may, by prior written approval from the GOO, or the 2IC/Campus Coordinator, be granted access to additional areas of the LTSA/LTU Network, in such a case, they must only access the Network for the purposes set out in the authority. Further, access to the Network may change without prior notice to team members.

Access to LTSA email accounts

Team members may only access the email account that is provided to them. No team member will be provided with access to an account other than their own email account.

Team members should note that LTSA and LTU's IT Service Provider will have the ability to access their email account for monitoring purposes.

Security of the LTSA/LTU Network

Team members are responsible for taking the appropriate steps to select and secure their password. Passwords should:

a) be unique from previous passwords;

b) be minimum of 10 characters long;

c) be complex, i.e. a mix of upper, lower, number, symbol; and

d) be changed every 90 days as per automatically directed to do so from LTU ICT Service.

If a team member suspects that their password or access code may have been disclosed or their account compromised, they should change all passwords and report the incident to the GOO without delay. LTU systems are targeted and phishing does occur from time to time. If a team member suspects that an email received is spam or may be an attempt to hack the system, ***DO NOT*** open it, just delete it. Any suspicious emails must not be opened however, if this does occur ICT Helpdesk must be notified immediately to change passwords by calling 1500 internally. The GOO must also be notified.

Accessing the LTSA/LTU Network away from the workplace

Team members can access the LTSA/LTU Network through the server, email through any device capable of email and VPN with a LTU VPN account when outside the workplace (including partial access if using a hand-held device).

When accessing the LTSA/LTU Network from outside the workplace, team members must comply with this policy. Remote access to and use of the Network will be monitored.

Confidentiality of information in the LTSA/LTU Network

a) Team members must handle all Confidential Information stored in or accessed through the LTSA/LTU Network in accordance with their contractual and legal obligations.

Personal Information

a) The LTSA/LTU Network contains Personal Information about individuals including students, clients and supplier contacts, consultants, team members and Contractors;

b) The Privacy Act 1988 (Cth) restricts the collection, use and disclosure of Personal Information. LTSA handles Personal Information stored in the LTSA/LTU Network in accordance with the Privacy Act and ***LTSA Privacy Policy;***

c) Team members are also required to comply with the ***LTSA Privacy Policy*** when handling Personal Information stored in or accessed through the LTSA/LTU Network. Any use of or access to photographs of LTSA personnel other than for the legitimate business purposes of LTSA is strictly prohibited without prior approval of the GOO.

Data Security

a) In addition to the ***LTSA Privacy Policy***, comprehensive technical measures are employed to protect information in the LTSA/LTU Network from unauthorised access. However, it may not always be possible to ensure the security and protection of Personal Information and Confidential Information when using the LTSA/LTU Network. Accordingly, team members should use their judgment when using the LTSA/LTU Network to store or communicate sensitive Personal Information or information that is highly confidential;

b) Team members should consider using more traditional means of communicating such information to its intended recipient, or the use of encryption.

Acceptable and prohibited use of the LTSA/LTU Network

LTSA provides the LTSA/LTU Network as a business tool. Personal use of the LTSA/LTU Network must be in accordance with this policy.

This policy facilitates compliance with applicable laws, helps to maximise the efficient use of LTSA 's resources and ensures the LTSA/LTU Network is protected from viruses and other security risks.

Team members must also comply with all directions from time to time from the GOO and LTSA’s Policies including, but not limited to, **Equal Opportunity**, **Anti-Bullying** and **Freedom from Harassment**.

All information that is entered into the LTSA/LTU Network must be, to the best of the team member’s knowledge, accurate.

Team members must not use the LTSA/LTU Network for any illegal or inappropriate purpose and must comply with all applicable laws including those which apply to the access and use of an IT system or data contained in or accessed through an IT system. Some specific prohibitions are listed below. This list is not exhaustive. Team members must always use common sense and best judgment in deciding whether an activity is appropriate given LTSA’s status in the LTU community.

Team members **must not** use any part of the LTSA/LTU Network:

a) to gain access to, download, save, store or transmit illegal or inappropriate content including material, which is sexually explicit, violent, obscene, offensive or disparaging of others on the basis of gender, race, disability, religion, nationality, sexual orientation, age, marital status or any other protected status;

b) to use or allow others to use LTSA's property (including Confidential Information and Intellectual Property) for any purpose not related to their work for or on behalf of LTSA;

c) to breach or facilitate the breach of any Intellectual Property including copying without authority any material that is subject to copyright, or making such material available to others to copy;

d) to engage in any act of plagiarism, including copying without authority the copyright material of any third party;

e) for advertising, including personal advertisements, solicitations or promotions, not related to the business of LTSA;

f) to engage in any commercial activity not related to the business of LTSA;

g) for the creation, storage or dissemination of destructive computer programs (e.g., viruses or self-replicating codes);

h) to copy, install, download, modify, adapt, reverse engineer, disassemble or decompile any software comprised in the LTSA/LTU Network, without the prior written approval of the GOO;

i) attempt to install (or attach) any software product, hardware or other devices to the LTSA/LTU Network unless specifically authorised to do so by the GOO;

j) for on-line gambling, betting or gaming;

k) to send a communication in someone else's name without their authority; or

l) to access, download, save, store, send or display from the internet (or any other source), or compose an email message or other communication containing, material (including but not limited to sexually explicit material) which:

   i. may offend, humiliate, or intimidate another person;

   ii. may result in another person feeling victimised, undermined or threatened; or

   iii. makes a reasonable viewer:

      - think less of a person who is the subject of the communication;
      - exposes a person to ridicule, hatred or contempt; or
      - injures a person in his or her trade, profession or financial standing.

   iv. in any other way may breach LTSA policy; or

m) infringes another person's rights in respect of the handling of Personal Information under the *Privacy Act 1988* (Cth).

Personal use of the LTSA/LTU Network

While the LTSA/LTU Network is a business tool, LTSA acknowledges that team members may need to send personal correspondence, use the internet, or send email using the LTSA/LTU Network for personal reasons from time to time. If team members use the LTSA/LTU Network in this way, they must comply with this policy.

LTSA can monitor the frequency of, and length of time an individual spends on, personal use of the LTSA/LTU Network. Excessive personal use is not permitted. Examples of excessive use may include:

a) excessive amounts of time spent on the internet;

b) sending mass mailing or chain letters, distributing electronic greeting cards or other non-work-related electronic communications, attachments or files;

c) printing multiple copies of documents (particularly in colour); or

d) otherwise creating unnecessary LTSA/LTU Network traffic.

Monitoring the use of the LTSA/LTU Network

The LTSA/LTU Network is monitored for security, traffic flow and content by LTSA and LTU.

By using the LTSA/LTU Network, team members consent to LTSA doing this as it relates to their use of the LTSA/LTU Network. This monitoring is continuous and occurs when the LTSA/LTU Network is accessed using any device, whether the team member is in the office or outside LTSA's premises (including from home).

All web browsing activities are recorded with details of every website address visited and these records are reviewed as required. LTSA and LTU logs all electronic communications sent or received including electronic communications which team members may send or receive in a personal context. The log records details of the sender, addressee, date, time, subject title and the fact of an attachment. Electronic logs are only accessed by LTSA and LTU's IT Service Provider or GOO in relation to specific matters when the need arises. Please contact the GOO for more information about access to email logs.

The GOO may access the email account of team members if they are not contactable or on leave, and there is a business requirement. During this process, email settings e.g., out-of-office messages and email redirections may also be adjusted.

Protecting privacy

To the extent that LTSA User's use the LTSA/LTU Network to send or receive Personal Information, LTSA collects that Personal Information as part of its routine monitoring processes. Other use of the LTSA/LTU Network, such as internet browsing, may result in LTSA collecting Personal Information about LTSA User's as an incident of standard system operating processes.

Personal Information collected in this manner may be used to protect, maintain and improve the LTSA/LTU Network and to investigate breaches of LTSA's policies. LTSA may disclose this Personal Information to service providers, agents and Contractors to help it do this. This may involve sending Personal Information overseas.

Team members may request access to any Personal Information LTSA holds about them and ask that it be corrected if they think it is inaccurate. LTSA will take reasonable steps to correct inaccurate information but may deny a request for access in some circumstances (for example, compliance with the Privacy Act).

Blocked access to certain parts of the LTSA/LTU Network

LTU ICT have systems to block delivery of certain electronic communications, both in-bound and out-bound, and blocks access to certain internet sites. Personal email correspondence may also be blocked by those systems. For example, LTU will block an email if LTU believes, or security software identifies, that the relevant email (or its attachment):

a) is spam;

b) potentially contains viruses or might otherwise result in interference with or damage to the LTSA/LTU Network;

c) is sexually explicit, defamatory or vilifies, discriminates, menaces, harasses or offends;

d) is or may be in breach of any of LTSA's policies, including this policy;

e) is over a certain size; or

f) contains material that may be LTSA's Intellectual Property or Confidential Information, is sensitive, or adversely affects (or might, if known to others, adversely affect) LTSA's reputation or professional standing.

The fact that an electronic communication or internet site is not blocked by LTU's systems does not necessarily indicate that LTSA deems that that content is appropriate or suitable for viewing or use on the LTSA/LTU Network.

Guidelines for emails and other forms of electronic messaging

Email and instant messaging are made available via the LTSA/LTU Network as a business tool. Their use involves risks such as:

a) once an email is sent, it is impossible to control what happens next;

b) it is not possible to guarantee the integrity of an email as it is relatively easy to alter the text in a manner undetectable to the recipient's eye; and

c) it is possible to reverse-engineer attachments to emails which may reveal unintended information.

Despite these risks, email and instant messaging is often treated more casually than other forms of written communication. Team members should never write anything in an email or instant message that would make the sender, receiver (or LTSA) feel uncomfortable or threatened in any way:

a) if considered inappropriate or defamatory by GOO, team members, LTU, the LTSA Governing Board of Directors or elected Student Council representatives;

b) to see reported on the front page of a local and/or national newspaper;

c) to be openly discussed in online forums;

d) to see reported in any form of social media, including LTU StalkerSpace; and

e) to be cross examined about in a hearing.

If a thought cannot be expressed in a way that passes these tests, it most likely means that the thought should not be expressed at all. Email creates a permanent record. Emails and conversation histories are backed up regularly and may be retrievable as evidence for subsequent proceedings even after they have been deleted.

Dealing with inappropriate emails

For the purposes of this section, an ***"inappropriate email"*** is an email or other electronic communication that contains material, links or attachments which a reasonable person would consider to be offensive or inappropriate, or potentially breaches this policy or other relevant policies implemented by LTSA.

If the inappropriate email is received from a team member, Governing Board of Directors or an elected Student Council representative, the recipient must inform the GOO immediately.

In addition, if recipients of inappropriate emails feel comfortable doing so, LTSA strongly encourages recipients to tell the sender that they do not wish to receive emails of this nature. If this is communicated verbally, a file note of the conversation should be made. If recipients of inappropriate emails respond via email, they should not reply to the original email, but should start a new email.

The file note or email response should be retained as a personal record and may also be required by LTSA.

a) If the inappropriate email is received from a team member, elected student representative, student or client: Inform the GOO as soon as possible. LTSA will endeavour to take steps to ensure the sender stops sending material of this nature to the relevant person.

b) If the inappropriate email is received from an external source: Never click on a link or reference contained in an email from an unknown source. If team members know the external sender, they must tell them that they do not want to receive emails of this nature.

Complaints

If any LTSA User receives a complaint about the LTSA/LTU Network or internet site, they should contact the GOO immediately.

Uploading files to the LTSA/LTU Network from an external device

Removable storage media devices must not be connected to LTSA's PCs, laptops or any other part of the LTSA/LTU Network. If it is necessary to save a file from an external source to the LTSA/LTU Network in any other circumstances, it should be attached to an email and emailed to a LTSA/LTU email address before being saved to an appropriate location.

All electronic data received or created during LTSA's business must be stored on a LTSA/LTU server where its confidentiality and integrity are protected by the systems in place at LTSA. Availability of data stored on LTSA/LTU's servers is assured using a scheduled backup regime.

In all cases that dictate the use of removable storage media, Confidential Information must be encrypted. Data stored on removable media should always be protected by encryption except immediately before transfer to another computer. The unencrypted file should be deleted immediately after the transfer is complete. Where possible the storage space used by the deleted file must be wiped clean.

Storing work files outside the LTSA/LTU Network

LTSA has no control over the security of any files stored outside the LTSA/LTU Network or the integrity of any device or system in which they are stored.

All electronic files created in the course of LTSA's business should remain solely within the LTSA/LTU Network at all times, except where it is necessary to email copies in the ordinary course of LTSA's business (for example, to students/clients) and should not be stored outside the LTSA/LTU Network unless authorised by the GOO. Remote access, should be used to access such files from outside the office whenever it is possible to do so.

Team members must avoid saving any files created during company business to any external File Hosting service. If it is necessary to share documents with students/clients or others outside LTSA, team members should use email (considering the issues relating to confidentiality).

Exceptions should be sent to the GOO for approval so that the organisation can keep a log of the data location, content and access details.

Loss or damage to LTSA's equipment

Team members are expected to use due care with mobile devices, notebooks and other equipment provided by LTSA.

If LTSA-supplied equipment (including a mobile device) is lost or damaged, it should be reported to the GOO as soon as possible. In the case of theft, this must also be reported to the police also.

LTSA’s ***Mobile Device Policy*** sets out expectations and responsibilities in relation to mobile devices.

Mobile Devices

A team member may be eligible for a mobile device if, in the view of LTSA, it is deemed necessary for the appropriate performance of their position.

This policy should be read in conjunction with LTSA’s ***Mobile Device Policy*** which contains important information about the use of both LTSA-supplied and privately-owned mobile devices.

Team members must always comply with this policy when using a mobile device supplied by LTSA, not only when accessing the LTSA/LTU Network.

Team members who own a personal mobile device can connect their mobile device to the LTSA/LTU Network if their mobile device has been configured to receive LTSA's email, enterprise applications and security policies (***Mobile Access***). This can be connected by contacting the 2IC/Campus Coordinator. Once a team member's mobile device has been configured for Mobile Access, the team member must:

a) maintain the most recent software updates on his/her/their mobile device to comply with security requirements. This includes the mobile device operating system and any App updates. Failure to maintain the latest version of the mobile device's operating system will result in it being disconnected from the LTSA/LTU Network until updates are applied;

b) Always comply with this policy when using Mobile Access. Team members who have a LTSA-supplied mobile device must comply with this policy at all times when using that device, not only when using Mobile Access;

c) comply with all directions of LTSA/LTU's IT Service Provider in relation to his/her/their LTSA-supplied device or use of Mobile Access;

d) complete any additional required training as determined by the GOO;

e) contact the GOO as soon as possible if his/her/their mobile device is lost or stolen, whether that mobile device is supplied by LTSA or a personal mobile device; and

f) not charge the purchase of any personal apps for his/her/their mobile device to any LTSA corporate credit card.

LTSA will remove Mobile Access from a mobile device (whether supplied by LTSA or a personal mobile device) for team members that do not comply with these requirements.

LTSA assumes no financial responsibility for any charges related to the contractual agreement between team members and their relevant carrier. If a team member is leaving LTSA, LTSA/LTU's IT Provider will remotely delete the configuration that refers to the LTSA/LTU Network and all LTSA data held on that team member's personal mobile device.

It is the team member's obligation to regularly back up all data on their mobile device such as photos, music and games. LTSA is not responsible for any loss of data as a result of a team member's mobile device being lost, stolen, broken or wiped. For iOS devices (iPads, iPhones) LTSA recommends backing up to the team member's home computer using iTunes. iCloud backup can be enabled for automatic backup. Team members will be responsible to purchase more than Apple's free iCloud backup allowance (currently 5GB) if they require additional storage. This is not covered as a company expense and must not be charged to any LTSA corporate credit card.

Breach of Policy

LTSA treats any breach of its policies or procedures seriously. LTSA encourages reporting of concerns about non-compliance and will manage compliance in accordance with the *Higher Education General Staff Award 2020*, National Employment Standards (NES), Disciplinary Policy and employment contract terms.

Governance

Related Policies & Procedures	• LTSA Code of Conduct • LTSA Social Media Policy • LTSA Privacy Policy • LTSA Equal Opportunity Policy • LTSA Anti-Bullying Policy • LTSA Freedom from Harassment Policy • LTSA Mobile Device Policy • LTSA Disciplinary Policy • LTSA Complaints Handling Procedure
Legislation Mandating Compliance	• Privacy Act 1988 (Cth) • Copyright Act 1968 (Cth)

	- Trade Marks Act 1995 (Cth) - Competition & Consumer Act 2010 (Cth) - Spam Act 2003 (Cth) - Age Discrimination Act 2004 (Cth) - Disability Discrimination Act 1992 (Cth) - Sex Discrimination Act 1984 (Cth) - Racial Discrimination Act 1975 (Cth) - Australia Human Rights Commission Act 1986 (Cth) - Anti-Discrimination Act 1991 (QLD) - Human Rights Act 2019 (QLD)
Policy Owner	Governance and Operations Officer
LTSA Governing Board of Directors Approval	09th August 2022
Review Date	15th March 2024
Version	3