logicalsolutions
Technology problem? Solved.

Acceptable Usage Policy

Logical Solutions 2020 Limited

Last updated: 17 November 2026

This Acceptable Usage Policy covers the security and use of all information and IT equipment, systems and services provided or managed by Logical Solutions 2020 Limited (“Logical Solutions”). It includes email, internet, voice and mobile IT equipment and services.

This policy applies to all Logical Solutions employees, contractors and agents, and to all users at our customers who use systems, hosted services or communications services provided or managed by Logical Solutions (together referred to as ‘individuals’).

This policy applies to all information, in whatever form, relating to Logical Solutions’ business activities, and all information handled by Logical Solutions relating to other organisations with whom it deals, including our customers.

It also covers all IT and information communications facilities operated by Logical Solutions or on its behalf.

Computer Access Control – Individual’s Responsibility

Access to IT systems provided or managed by Logical Solutions is controlled by the use of User IDs, Passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals, and consequently, individuals are accountable for all actions on those IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any IT system provided or managed by Logical Solutions.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else’s user ID and password to access any IT system.
- Leave their password unprotected (for example, writing it down).
- Perform unauthorised changes to IT systems or information.
- Attempt to access data they are not authorised to use or access.
- Exceed the limits of their authorisation, or specific business need to interrogate the system or data.
- Connect any unauthorised device to the network or IT systems.

- Store business data on any unauthorised equipment.
- Give or transfer business data or software to any person or organisation outside their organisation without appropriate authority.

Managers must ensure that individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

Internet and Email Conditions of Use

Use of internet and email services provided or managed by Logical Solutions is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Logical Solutions or its customers in any way, is not in breach of any term and condition of employment and does not place the individual, Logical Solutions or its customers in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images) which is offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect their reliability or effectiveness, for example, distributing chain letters or spam.
- Place any information on the internet that relates to their organisation, alter any information about it, or express any opinion about it, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward business email to personal email accounts (for example, a personal Hotmail account).
- Make official commitments through the internet or email on behalf of their organisation unless authorised.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.

- Download any software from the internet without prior approval of the IT department or Logical Solutions.
- Connect devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, a clear desk and screen policy applies as follows:

- Personal or confidential business information must be protected using security features provided, for example, secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken not to leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must comply with the applicable remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example, at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile storage devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only authorised mobile storage devices with encryption enabled may be used when transferring sensitive or confidential data.

Software

Individuals must use only authorised software on computers provided or managed by Logical Solutions. Authorised software must be used in accordance with the software supplier's licensing agreements. All software must be approved and installed by Logical Solutions or the authorised IT department.

Individuals must not:

- Store personal files such as music, video, photographs, or games on business IT equipment.

Viruses

Logical Solutions implements centralised, automated virus detection and virus software updates on the systems it manages. All managed PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of business voice equipment and services is intended for business use. Individuals must not use business voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communication. Use of flat rate voice services is also subject to our Fair Use Policy.

Individuals must not:

- Use business voice services for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or international operators unless it is for business use.

Actions upon Termination of Contract

All business equipment and data, for example, laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the organisation that owns them at the termination of the contract or employment.

All business data or intellectual property developed or gained during the period of employment or engagement remains the property of the organisation and must not be retained beyond the termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on business computers is the property of the organisation that owns those systems. Wherever possible, personal emails will not be opened.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Logical Solutions has the right (under certain conditions) to monitor activity on the systems it provides or manages, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes and New Zealand law, including the Privacy Act 2020.

This policy must be read in conjunction with:

- the Privacy Act 2020;
- the Crimes Act 1961 (including its provisions on crimes involving computers);
- the Harmful Digital Communications Act 2015;
- the Unsolicited Electronic Messages Act 2007;
- the Copyright Act 1994; and
- our Privacy Policy.

It is your responsibility to report suspected breaches of security policy without delay to your manager, your IT department or the Logical Solutions helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the relevant organisation’s disciplinary procedures, and Logical Solutions may suspend or restrict access to the affected services.