



EMAIL, INTERNET AND SERVER USAGE POLICY

Intelligent Training Solutions Pty Ltd

ABN 25 151 191 669

Policy Documentation

Document No:

1. VERSION CONTROL:

Version	Document No:	Date	Author	Reason	Sections
1.0		11/12/2012	AM	Initial Release	<All>
1.1		11/12/2012	AM	Error Identified	Header

2. AMENDMENTS IN THIS RELEASE:

Section Title	Section No:	Amendment Summary	Ver
ALL	ALL	Review and Update Signatures	1.1
Header		Document header identified as incorrect. Correction made to the header section of this document	1.1

3. DISTRIBUTION:

Copy No	Version	Issue Date	Issued To
1	1.0	11/12/2012	Training Manager
2	1.0	11/12/2012	All Staff via Email
3	1.0	11/12/2012	All Staff via Server
4	1.1	11/12/2012	All Employees and Contractors via Server

Uncontrolled when printed

Intelligent Training Solutions ACN 151 191 669

EMAIL, INTERNET AND SERVER USAGE POLICY

1. Purpose

Intelligent Training Solutions Pty Ltd is committed to managing Information Technology (IT) risks inherent in our operations and to provide safe systems of work to prevent personal or business exposure to risk, reputation or property damage.

In keeping with this commitment ITS has adopted the "Email, Internet and Server Usage Policy. This is in line with the company's obligations under the Privacy regulations.

The use of email and internet has become an essential business tool for most employees and contractors; however the inappropriate use of email or internet can cause a distraction or impact on other persons within the workplace.

Employees and contractors are permitted to use Internet E-mail for occasional or incidental private purposes but should be aware that they will be subject to this Policy.

2. Definition

3. Objective

To ensure IT equipment is used within its intended purpose and within the protocols of this Policy

4. Scope

This policy applies to any person using an ITS computer, laptop, PDA, Tablets PC or whilst under the management control of ITS or conducting activities on behalf of ITS where its reputation may be negatively impacted.

5. Email

General Conditions of Use

Access to Internet E-mail is granted on the basis that it is primarily used for business purposes related to the job function of the Employee.

Employees are permitted to use Internet E-mail for occasional or incidental private purposes but should be aware that they will be subject to this Policy.

Ownership of Copyright

Intelligent Training Solutions Pty Ltd ("ITS") retains the copyright to all material created by its Employees.

Privacy of Electronic Mail & Right to Access Business & Records Created by Employees

ITS respects the rights of its employees and contractors to privacy. ITS routinely monitors the E-mail and Internet usage, including sites accessed, and the duration of such access. ITS reserves the right to access the contents of any:

- Electronic mail sent or received by any employees or contractor, whether for business purposes or not; and
- Data file, word processing document, or any other computer documents created by an employee or contractor, whether for business purposes or not;

For the purposes of:

- (a) Retrieving files for system maintenance;
- (b) Investigating and monitoring any suspected improper conduct on the part of any employee or contractor; or
- (c) Complying with a court order.

Prohibited Contents of E-mail Messages

To protect both ITS and its employees and contractors against litigation, and to ensure other staff are not subjected to offensive material, Employees and contractors are prohibited from including the following material in any E-mail messages:

- Material which may be defamatory;
- Material which may breach copyright laws;
- Material containing sexual comments;
- Material containing religious statements or opinions;
- Material containing political statements or opinions;
- Material that may be sexually, racially or in any other way discriminatory;
- Any other objectionable material, including, but not limited to, pornography of any kind, sexually degrading material, material depicting violence, material containing foul language or any material that provides instructions on the commission of violent crimes;
- or
- Material prejudicial to ITS interests.

In order to protect the Company's corporate image, all email communications should take a professional tone.

To protect both ITS, its employees and contractors and to ensure other staff are not subjected to offensive material, Employees and contractors are prohibited from circulating any E-mail messages that include any material as listed above and chain letters.

Employees are also strictly prohibited from sending Email messages containing ITS data to the Company's competitors.

Employees must not remove or transfer ITS data from their hard drive via media outlets such as USB or CD without obtaining prior approval from Company Directors.

User Accountability

Employees and contractors must choose unique passwords (no personal or work details) that must be changed regularly (i.e. every 3 months when prompted). Upon request, Employees and contractors must disclose their individual password(s) to all electronic communications systems to the Training Manager, CEO or the IT officer. Individual passwords must not be revealed to any other co-worker or third party. If Employees and contractors need to share information with colleagues or third parties to conduct Company business they should use authorized information-sharing mechanisms (e.g. email, FTP Services).

E-mail Subscriptions and Other Internet Services

Unless relevant to business, Employees and contractors are not entitled to subscribe via E-mail to free services such as hobby groups or discussion groups.

Client/Customer Inquiries

In order to maintain a high level of service, all E-mail messages received from clients/customers ("customers") must be replied to within 24 hours, acknowledging receipt of the message and setting out what action is being taken.

As part of ITS's policy on customer complaints, any customer complaints received via E-mail must be forwarded to a Training Manager or Program Coordinator.

When Out of the Office

If you will be absent from the office for an extended period, such as for annual leave, you must arrange:

- to have your E-mail automatically forwarded to another staff member; and
- to automatically send a reply stating when you will be back in the office.

E-mail Document Management

It is imperative that copies of all E-mail correspondence are retained as an electronic copy and backed up on the ITS Server or company created dropbox folders.

Computer Viruses

It is possible for computer viruses to be transmitted from attachments to E-mail messages. If you receive an attachment from someone you do not know or trust, it must be forwarded to the IT admin officer for virus checking.

Any E-mail message received informing you about any virus must be forwarded immediately to the IT admin officer for investigation.

Employees and contractors are prohibited from connecting personnel storage devices to the ITS network without prior approval and scanning from the IT admin officer or Training Manager.

Failure to follow the E-mail policy could result in restrictions being placed upon its use, including withdrawal of private use rights, and possible disciplinary action.

Employees and contractors are prohibited from modifying the Company's IT security settings at all times.

Information Sensitivity

Employees and contractors are reminded that most electronic communications systems are not automatically encrypted. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. All information sent externally which is of a sensitive nature must be sent in a format that cannot be modified.

Unless an employee is using a data encryption technique, at no time should electronic communications system be used to forward confidential information outside of the Company without the specific authorisation of the Training Manager or CEO.

6. INTERNET

General Conditions of Use

Access to the World Wide Web is granted on the basis that it is primarily used for Employer business purposes, for research or for other activities related to the job function of the Employee and on the approval of the Training Manager or CEO.

The web sites accessed may be monitored and sites accessed with no business relevance to ITS may be denied. Inappropriate Internet activity may result in access being taken away, disciplinary action or termination.

Employees and contractors are not entitled to publish a web page without prior approval.

Security

Security on the Internet cannot be guaranteed unless specific encryption software has been installed by both ITS and the other party/parties involved in the communication.

Downloading Material from the Internet

Employees and contractors are permitted to download information related solely to ITS's business activities but must conduct virus checks (see section 5. Computer Viruses).

To avoid software licence infringement and to maintain the integrity of our computer systems, Employees and contractors are prohibited from downloading any software applications or other executable file, including any demonstration software, without the prior approval of a Training Manager the CEO.

Employees are prohibited at all times from storing personal music files and videos on the ITS network. Employees are prohibited at all times from downloading any of the prohibited material as set out in section 5, Prohibited Contents of E-mail Messages.

Prohibited Activities whilst Utilizing the Internet

To protect ITS, its employees and contractors against litigation, Employees and contractors are prohibited from posting the following material online at work or from a ITS computer at any time:

- comments which may be defamatory;
- comments which may breach copyright laws;
- comments containing sexual comments;
- comments containing religious statements or opinions;
- comments containing political statements or opinions;
- comments that may be sexually, racially or in any other way discriminatory;
- any other objectionable comments, including, but not limited to, pornography of any kind, sexually degrading comments, comments encouraging violence, foul language or any instructions on the commission of violent crimes; or
- comments prejudicial to ITS's interests.

Dated: 01st May 2018

_____ *[sign]*

Alexander Mueller

Director and Chief Executive Officer

Intelligent Training Solutions Pty Ltd