

INTOWORK AUSTRALIA IT USAGE GUIDELINES

The Corporate Wide Area Network (WAN), intranet, Internet, electronic mail (email), carriage services / devices (mobile), desktops, laptops, video conferencing and Instant Messaging (IM) are important business and educational tools that can enhance workflow and employee learning, increase productivity and help users perform a variety of tasks; as such they should be used in an efficient, lawful and ethical manner.

The IntoWork IT Acceptable Usage Guidelines have been developed to expand on the IntoWork IT Acceptable Usage Policy. These documents have been developed to provide awareness of personal accountabilities for IntoWork Group staff in what is acceptable and unacceptable usage of IntoWork IT physical assets, devices, networks and operating systems. The desired outcome of these controls is that the safety and integrity of information technology infrastructure and software platforms are not impeded or negatively impacted in any way through the misuse of the company's Information Systems.

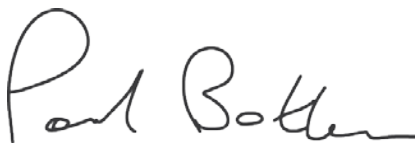
These documents also aim to deliver transparency to end users of IntoWork Information Systems in communicating the level of monitoring, surveillance and auditing that occurs within the company's Wide Area Network.

IntoWork Australia is committed to continual improvement in the area of proper and appropriate information technology usage through a process of policy review and evaluation.

These guidelines apply to all users of IntoWork Australia's and IntoWork Group businesses facilities, including all IntoWork Group employees, students, apprentices, trainees, all contracted service providers with access to IntoWork Australia or IntoWork Group business information technology infrastructure.

Associated Documents:

- IntoWork Australia IT Usage Policy

A handwritten signature in black ink that reads "Poul Bottern".

Poul Bottern
Group CEO

04 March 2019

GUIDANCE NOTES

User Responsibility

All users are expected to take reasonable precautions to protect WAN, intranet, Internet, email, mobile, video conferencing and IM systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.

This may include but not be limited to:

- Not allowing any other individual to use your named network account.
- Not using another user's named network account.
- Not providing or allowing unauthorised access to information.
- Maintaining security, complexity and confidentiality of user ID's and passwords.
- Not providing network user IDs and passwords to any other party including IntoWork IT staff or third party IT Contractors.
- Not maintaining an insecure hard copy of network or IntoWork application passwords.
- Changing of passwords where it is suspected that account security may have been compromised or accessed by another user.
- Ensuring company electronic records of continuing value are not destroyed prior to their capture on the appropriate IntoWork IT endorsed company record-keeping system.
- Reporting of any damage, to either hardware or software, to IntoWork IT immediately.
- Reporting of any identified or supposed security vulnerabilities or breaches to IntoWork IT immediately.
- Maintaining of confidentiality with reference to any personal information accessed via the IntoWork Corporate WAN and Business Information Systems as outlined in the Notifiable Data Breaches Scheme, relevant Privacy Legislation and the IntoWork Privacy Policy.
- Maintaining of confidentiality with reference to company and commercial in confidence information accessed via the IntoWork Corporate WAN and Business Information Systems.

Acceptable Use

Any information systems provided on a company network or any information technology infrastructure, equipment or devices provided by the company can only be used for its intended purpose. I.e. business purposes.

Business use includes any activity that is conducted for purposes of accomplishing official business, professional duties including research and, where appropriate, professional development.

Users will be held personally accountable for any use of the company's WAN, intranet, Internet, email, mobile, video conferencing, devices and IM services that does not comply with these principles.

Personal Use

The company accepts that employees may on occasion use company IT assets and IT information systems and networks for incidental and limited personal purposes. Employees must at all times ensure that any personal use of IT devices and services are both economical and ethical. They must ensure such use does not:

- Interfere with performance of the IntoWork network or any other user's IT experience.
- Generate any additional financial costs for the company

- Interfere with personal employment performance

Staff are not permitted to use company IT devices or services for:

- Unauthorised commercial activities
- Unauthorised personal gain
- Unauthorised access / gain for third parties

Inappropriate Use

Examples of inappropriate use of WAN, intranet, Internet, email, mobile, desktops, laptops, video conferencing and IM include but are not limited to:

- Disrupt or interfere with the use of WAN, intranet, Internet, email, mobile, video conferencing and IM services.
- Execute unapproved applications, software or executable scripts.
- Download software, without appropriate authorisations being documented and data security / licensing requirements being complied with.
- Attempt to intentionally access any secure area of the WAN whereby explicit access has not been granted.
- Attempt to modify any aspect of the WAN or information technology system / environment which is centrally managed by IntoWork IT.
- Make copies or distribute copies of company software.
- Use IT systems for duplication of copyright material.
- Save personal data such as digital music, videos or photographs to company devices, servers and WAN locations.
- Disrupt communication and/or information technology performance through personal use of IntoWork IT services and/or resources.
- Access inappropriate and/or offensive, non-business related Internet sites.
- Download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet sites.
- Download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, sexual orientation, ethnicity or religious and political positions and beliefs.
- Distribute defamatory, obscene, offensive, bullying or harassing messages to other IntoWork end users or members of the general public.
- Distribute confidential information without explicit authority.
- Distribute private information about other end users or members of the general public without explicit authority.
- Register with websites or organisations using company email addresses unless specifically related to company business.
- Without authority destroy, alter, dismantle, prevent rightful access to or otherwise interfere with the integrity of IT equipment/hardware, intranet, Internet, email, mobile services, video conferencing or IM services.
- Without authority destroy, alter, dismantle, prevent rightful access to or otherwise interfere with the integrity of IntoWork digital folders, files and database records.
- Intentionally open, reply to or forward illegitimate non-business related email using IntoWork Electronic Mail Clients and Servers.
- Make intentional attempts to bypass IntoWork IT security, monitoring and inspection or content filtering systems.

Recordings

'Recordings' include photos, voice recordings and video recordings, but excludes video surveillance via company CCTV systems.

Electronic devices with recording capabilities must not be used in any place where a recording device would normally be considered inappropriate by a reasonable person. This includes in change rooms and toilets or any situation which may cause embarrassment or discomfort to others.

Recordings of person/s at company premises, or of person/s performing an activity or function directly associated with company operations (irrelevant of who owns the recording device), are not permitted unless:

- the person/s being recorded have been explicitly informed of the recording, prior to partaking in the recording; and
- no person/s being recorded overtly object to the recording; and the recording is lawful.

Any such recordings must not be published in a public forum (for example, posted to a website or to social media) without express permission being obtained from those recorded, prior to distribution.

In addition, prior to recording, the company must obtain written consent from the person/s being recorded (or if the person/s being recorded are under 18 years of age, their parent/guardian), if:

- the recording is intended to be used by the company for the purpose of public relations, promotion, advertising, media or commercial activities; or
- the recording is intended to be posted online or published in any public forum.

Data Management

Data quotas that are implemented shall be enforced. This includes but is not limited to network folder size, electronic mailbox size, email attachment size limitation, My Documents and U:\ drive, SharePoint Online and OneDrive storage space.

IntoWork Australia will not be responsible for loss of personal data, images or files that have been stored on IntoWork hard disks, storage devices, mobile devices or WAN locations.

Monitoring & Inspection

The company reserves the right to monitor any or all WAN, server, intranet, Internet, email, mobile, video conferencing and IM systems related activity and to monitor and inspect any or all email messages and IM chat logs sent or received by users of company IT resources, in order to:

- Identify inappropriate use.
- Identify cyber-bullying.
- Protect system security.
- Maintain system performance.
- Modify content filtering.
- Determine compliance with contracts, legislation and company policy.

These monitoring and inspection activities include but are not limited to the following:

- Access and examination of specific types of messages e.g. large messages or messages containing executable, audio visual files, movie files, command files and/or pictures, in order to identify inappropriate use or to maintain system performance.
- System security auditing.
- File and folder access and handling auditing.

- Access and examination of messages in specific circumstances, such as where an individual's message volume is high or at the peak periods of the year or on a random sampling basis, in order to identify inappropriate use or to maintain system performance.
- Monitoring and inspection can apply to personal, business or educational use of WAN, intranet, Internet, email, mobile, video conferencing and IM systems and personal, business-related or education-related email messages delivered via the IntoWork Corporate WAN and associated information technology systems.
- Account login history.
- Internet browsing history.
- Print and photocopier usage.
- Hardware monitoring.
- Remote access / viewing of active computer screens / monitors.
- Video surveillance

Consequences of Policy Violations

Violations of this policy by employees may lead to disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

Violations of this policy by students may lead to:

- Disciplinary action.
- Request for reimbursement of expenses resulting from malicious acts or purposeful damage.

Compliance

IntoWork Australia Executive Manager of Information Technology is responsible for implementation, maintenance and review of this policy.

All individuals within the Scope of this policy have a moral and in some cases legal obligation to comply with the above usage policy guidelines and are responsible for ensuring that this policy is adhered to.