Policy on acceptable use of information and communications technology

# Purpose

This policy on acceptable use of information and communications technology (ICT) establishes guidelines for the correct use of Infoxchange’s technology - including email, internet, social media, personal computers, tablets and telephones.

If you have access to Infoxchange’s ICT systems, you must know about, understand and comply with this policy.

All staff must comply with this policy at all times. That means you have to:

* use systems lawfully
* avoid viruses and offensive material
* remember you are at work
* keep information secure on all devices including laptops and phones
* not share individual accounts and keep passwords secure
* manage administrative accounts securely
* waive your right to privacy
* report breaches of security.

# Use systems lawfully

Under Australian and New Zealand law, the individual may be responsible for any breaches of anti-discrimination legislation. This means you must never use Infoxchange’s computer or communication systems to harass, bully or discriminate against anyone. You must also never use those systems to breach software licencing or copyright laws by pirating material or sharing pirated material.

# Avoid viruses and offensive material

You must take care to avoid and not distribute electronic material that may be harmful to the organisation, staff, clients or others, or to the information and communication system itself. Don’t use or share:

* technologically harmful material (such as viruses and malware)
* material which is sexually explicit, harassing, fraudulent, obscene, intimidating, defamatory, racist, sexist, abusive, discriminatory, threatening or otherwise offensive.

Sending, receiving, displaying, printing or otherwise disseminating material which is fraudulent, illegal, sexually explicit, obscene, intimidating, defamatory, racist, sexist, abusive, discriminatory, threatening or otherwise offensive is prohibited. You must not knowingly share or distribute such material.

Do not open any attachments or click on any links provided in an email unless you are confident about the identity of the sender and sure that the content is acceptable for work use.

All files from email, removable media or the web must be virus scanned before you open them.

If you inadvertently download or access harmful content, don’t panic, but don’t pretend it didn’t happen.

* If you suspect you have a virus or malware, stop using your computer and immediately let your ICT support staff know.
* If you’ve opened material that could be offensive to others, delete it or close the relevant web page/program(s) and report the material to your manager immediately.
* If you know the person who sent the virus or offensive material, tell the sender the material is harmful or inappropriate nature and ask not to be sent such material again.

# Act professionally and appropriately

Infoxchange recognises that staff members sometimes need to use technology for private reasons. This use is nevertheless a privilege: don’t do it too often or for too long. If your internet, email or phone use could be seen to be impeding your ability to carry out your work, or if it’s affecting the organisation, it may be deemed ‘excessive use’ and your privilege could be revoked.

Your ICT use must not negatively affect Infoxchange’s good reputation, data security, or the safety or well-being of clients or other staff. This rule applies whether you’re using Infoxchange systems as well as personal resources, within work hours as well as out of office hours - your personal use of ICT should not affect Infoxchange’s reputation. You may not use Infoxchange’s (or client’s, where relevant) ICT resources for advertisements, solicitation or promotions that are not related to Infoxchange’s business.

**You are personally responsible for the content you publish in a personal capacity** on platforms such as public websites, social media and the like. Where your comments or profile could identify you as an Infoxchange employee, you must clearly state that the comments are your own and are not those of the organisation, and you must conduct yourself so as to not adversely affect the organisation or its associates.

**Only authorised staff may comment or set up online accounts (such as social media) on behalf of the organisation.** To become authorised to comment you will need prior approval from your line manager as well as from Infoxchange’s communications manager.

Take care when using electronic communication such as email to send information. Once it’s sent, you have no control over where it may end up. Include a disclaimer on all emails to impose a duty of confidentiality on whoever gets the email. For example, you could use this standard text:

* *EMAIL PRIVACY DISCLAIMER: The contents of this e-mail, including any attachments, are intended only for the person or entity to which this e-mail is addressed and may contain confidential, and/or privileged information. If you are not or believe you may not be the intended recipient any disclosure, copying or use of this information is prohibited. If you have received this e-mail in error or have concerns regarding its transmission please advise the sender immediately by return e-mail, delete this e-mail and destroy any copies.*

If you get an emails or other correspondence in error, tell the sender immediately and then delete it. You must not forward it on to other people.

# Keep information secure on all devices including laptops & phones

*Note: This section covers both your own devices used in the course of your work with Infoxchange and any devices provided by Infoxchange.*

**Store work data on the server wherever possible**, not on a personal device such as a computer, tablet, phone or external hard drive. If data is stored on the server it is automatically backed up and protected against disk failure. Storing data this way also prevents the security risk of sensitive data being exposed in the event of a theft or loss.

In instances where you need to store confidential Infoxchange information and data on personal computing devices, data storage, mobile devices or other systems, you must take due care to protect this information from loss and theft.

* Make sure desktops and laptops are configured so you have to sign in with a complex password (refer to section 6 below) to access stored information, and that the computer asks for the password after 15 minutes of inactivity.
* For **smartphones and tablets** (even those you own) that are configured to access email and other organisational information, make sure the device:
  + can be **remotely wiped** if you lose it
  + has a secure access passcode that auto-locks after no more than **five minutes** of inactivity.
* **Never leave equipment unsecured**, including visible in a car or unprotected in a conference area.
* **Immediately tell** ICT support and your manager if your computer or device is **lost** **or stolen.**
* If you must use an **external hard drive or USB flash drive**, make sure any information you store on it is:
  + not confidential, and poses no risk to the company if it becomes available publically, **or**
  + secured with a complex password that cannot be readily breached.

If you are in doubt, do not store data on potentially insecure devices.

* If you use a Linux, Mac or Windows 8 **laptop**, ensure that **full disk encryption** is enabled and working.
* Don’t use **personal** accounts to store Infoxchange information **in the cloud** via services such as Dropbox or Google Drive.You can use organisational accounts approved by the Corporate Services Manager.

When you use your personal PC to access organisational information, you are responsible for making sure the computer has appropriate security protection in-place. This means your computer or device should require entry of a **complex** **password** to access the information (see the bullets above and section 6 below), and be covered by current **antivirus protection** (on Windows computers) that it is up to date with security updates and patches. (If you are using your personal PC to **store** confidential information, **all** the above bullet points apply).

If you are using a **public computer,** make sure **no company information is saved on the computer.** (This excludes temporary internet files; do not save files or attachments to the hard drive.)

# Don’t share individual accounts and do keep passwords secure

You will be given individual passwords and logins so you can use various ICT systems. **You are accountable for all activity that occurs in an ICT system under your login, so make sure your login information is kept secure**.

Only use your own login to access Infoxchange systems. (The exception is if you have an administrative account; this is described in the section below.)

Do not share your login information with anyone except systems staff, who may ask for this information so they can install software or perform maintenance tasks within your account. Once they’re finished, change your password immediately.

Please follow these principles to maintain security:

* Change your organisation-issued password the first time you sign in.
* Make passwords complex: at least eight characters long and with a mix of upper and lower-case letters, numbers and special symbols such as ! @ #.
* Change your password regularly (about every 60 days).
* Never write your password down.

# Manage administrative accounts securely

Some staff are allowed to access administrative accounts, for example:

* **internal administrative accounts** used to administer Infoxchange’s infrastructure and systems, such as servers and client management software
* **other shared accounts** used on external websites for functions such as banking, ordering, incident logging and so on.

Limitations in the underpinning technology mean that these administrative accounts are shared.

These accounts must be controlled to make sure security risk is appropriately managed (particularly in the event of staffing change). All managers/team leaders are responsible for:

* maintaining a list of all shared accounts/passwords and the individuals in their team who have access to them
* securely storing this information in an encrypted format
* undertaking a risk assessment in the event of a staffing changeover and changing shared passwords when appropriate.

# Waiving your right to privacy and information ownership

Electronic information you create, send or receive using Infoxchange’s communications technologies is the property of Infoxchange. As such, Infoxchange has the right to monitor any and all aspects of its computer system including, but not limited to, internet sites you visit, files you download and upload, and email messages you send and receive using Infoxchange’s email accounts.

Subject to any applicable telecommunications and privacy laws, you waive any rights to privacy that you may have in respect of anything that you create, store, send, or receive on or through Infoxchange’s ICT system.

Remember that although access to ICT systems is password protected, authorised staff can still access it. You should be aware that your line manager or others as directed by the CEO may access your accounts if it is deemed necessary.

# Report all security breaches

You must notify your line manager immediately of any content or activities you find which contravene this security policy or which may otherwise pose a risk to the security of Infoxchange’s ICT system.

# Compliance

All Infoxchange staff and anyone who uses Infoxchange’s ICT resources must comply with this policy at all times.

Improper use of organisational resources may threaten the system’s security, the safety and wellbeing of staff and others, and the liability, profitability and success of the organisation.

As such, if you fail to comply with the policy it may result in disciplinary action. In serious circumstances, you could be dismissed or have your employment agreement terminated.