## A-Z Guide

# Information Communications Technology Policies

## Contents

# Overview

- Information and communications technology policies (ICT policies) are those policies that explain to your employees the intended use of all of your organisation's information and communication technology, and what will constitute misuse and abuse.
- ICT policies should address the protection of property rights and personal rights that are created wherever and whenever ICT is employed.
- ICT policies can be drafted so that they succinctly encapsulate the technology your organisation currently uses, and the technology that it is likely to invest in, in the future.
- ICT policies should be living documents that are realistic, manageable, and enforceable; to this end they should reflect your "house rules" and/or employment agreements, be consistent with your organisation's other policies and procedures and reflect your ongoing workplace practices.

# Introduction

This A-Z Guide addresses the protection of personal rights and property rights that comprehensive information and communications technology policies (ICT policies), should cover. It is up to your organisation to assess whether one policy can cover everything or whether a multiple of specialist policies are needed.

As technological advances occur, and personal and property rights develop in response to those advances, it is possible to keep abreast of the change and its implications without revisiting your policies every time a new product appears on the market. So long as your policies are drafted to capture the essence of personal rights and property rights in a way that makes it clear that your organisation seeks to protect these, then you will find that the policy works for the organisation.

Having said that, as with all policies, ICT policies need to be living documents. They have to keep pace with change generally, but more importantly they need to reflect the changes that occur from time to time in your organisation. ICT policies should be accessible, realistic, understood, and enforceable; it may be necessary to review on a regular basis.

Before drafting your ICT policies you will need to consider:

- The nature of your business and how the work is done;
- The sort of access to your ICT you provide customers, employees and others with;
- The sort of ICT you use and what it is capable of;
- The sort of damage that could be done to your organisation by misuse or abuse of ICT;
- The extent to which your organisation is dependent on ICT;
- What resources your organisation can devote to policing its policies; and
- Who in your organisation is able to provide advice on ICT.

# Application

When we talk about ICT, what exactly do we mean? In this A-Z Guide it refers to everything related to information and communications technology. It includes hardware, software, and infrastructure. These examples are illustrative and not exhaustive.

**Hardware:**

- Computers, including PCs and laptops
- Servers
- Phones, mobile phones and VOIP (e.g. Skype)

- Hand-held computers
- Pagers
- Presentation technologies

**Software:**
- Web browsers
- Applications (e.g. Facebook, Twitter, data cleaning programs, online chat programs)
- Email
- FTP browsers
- Computer to computer communication
- Computer to phone communication

**Infrastructure:**
- Networks
- Cable
- Wireless
- Optical

# Potential Exposure

There are a number of ways in which your organisation can be damaged by the misuse and abuse of its ICT. The damage might not be direct; your organisation could be held liable for damage that is done to another organisation or person. So, when thinking about email and internet policies, you need to think about the potential for damage both inwardly and outwardly.

## Reputation

The reputation of your organisation will be important to you. Your suppliers, customers, and employees expect to have confidence in your organisation's ICT. A serious breach of any of your ICT, particularly if it concerns an external party, could, if it becomes known, adversely affect your reputation, and may discourage other organisations from doing business with you.

## Property rights

Your organisation needs to protect its property; the circumstances will dictate what property owned by your organisation is at risk and therefore needs to be protected by ICT policies. It is important to understand that property rights exist in respect of:

- Hardware
- Software
- Copyright
- Trade Marks
- Patents
- Information
- Licences and contracts

However, not only your property rights are at risk when people, particularly employees, use ICT at work. The property rights of other organisations and people, most commonly via the internet, are also at risk. As an employer you can be held liable for the acts of employees so you will want to draft your ICT policies to address this. Property rights can also be at risk when employees work from home, whether they are using your equipment and software or their own.

The damage in respect of property rights may be physical or actual, and/or financial. Hardware may be damaged by carelessness or sabotage; software licences and copyright may be infringed by unauthorised copying or sharing; confidential or commercially sensitive information may be leaked, taken, damaged, or destroyed by viruses, hackers, ignorance, and downloaded programmes; trademarks and patents may be infringed by unauthorised use.

## Employment rights

Every employment relationship is dependent on trust and confidence; the duty, which applies to employers and employees, obliges both parties to behave in a manner towards each other that does not damage the relationship. Employers are entitled to expect that their employees will work only for them, and that their employees will not conduct themselves in a manner that is against the employer's best interests. In this context, employers have "rights" in respect of:

- Confidentiality
- Time
- Performance
- Conduct
- Indemnity

Employees, on the other hand, are entitled to expect that their employers will preserve their right to individual privacy, and that they will be treated fairly. In this context, employees have "rights" in respect of:

- Privacy
- Fair treatment
- Safety

Your policies need to take into account each party's respective "rights" by being open and upfront about what is and is not expected, and what could happen in either case. It is important for employers to "set the tone" for the workplace in terms of what is acceptable use. For example, you may not wish to ban all email "forwards" but only those which could be considered discriminatory/harassment or otherwise unlawful.

Likewise, you may want to restrict access to social media completely, or to outside work hours, or allow access at work provided it does not interfere with performance and the use does not otherwise breach your ICT policy.

## Copyright (Infringing File Sharing) Amendment Act 2011

Employment rights might also be affected under the Copyright (Infringing File Sharing) Amendment Act 2011 which comes into force on 1 September 2011. The Act establishes a three-notice regime to deter illegal file sharing. This process involves copyright infringers being issued with a 'detection notice', followed by a 'warning notice' if the infringement continues or there is a further offence, and finally an 'enforcement notice'. The Act also extends the jurisdiction of the Copyright Tribunal, enabling it to hear complaints and award penalties of up to $15,000. Under the Act, Copyright owners may also seek suspension of an internet account for up to six months through the District Court. This Act could impact on workplaces where the internet is accessible by employees as there is the potential for infringement file sharing and therefore, for the company's internet account to be suspended. This should be addressed as part of the company's ICT policy.

Refer to the **A-Z Guide** on **Illegal File Sharing** for more information

# Drafting Policies

The first thing to consider when contemplating the contents of your organisation's ICT policies is how your organisation is going to enforce them. There is no point, for example, banning all personal use of the computers, if it is not going to be possible to police this. Nor is it sensible to do this, if exceptions are going to be made. The next thing to consider is the proper use of something, and then what improper use could constitute.

It is also very important to ensure that your ICT policies complement, and not contradict, any of your other policies. They should be consistent with your company rules (house rules) and your employment agreements. Your policies should provide a guideline of the investigatory processes and disciplinary processes your organisation has adopted. A clear indication should be given of the consequences of breach of the ICT policy and this should be enforced consistently.

## Property rights

Your organisation has a right to protect its property rights in its ICT; it has the right to protect it against misuse and abuse by whatever means it deems reasonable, appropriate, and justified. A number of electronic security options are available now, and new ones are being developed all the time. Firewalls, port scanning, anti-virus software, and automatic inventories are just some ways of enhancing your organisation's electronic security.

It is important to be clear in your policies about what property rights your organisation wants to protect; this clarity can assist people to understand why your organisation has chosen to undertake the security measures that it has. It is also important to make it clear in your policies what use of any ICT is permitted, and what use is not; however you do not want to make these descriptions exhaustive, but rather illustrative, so that the policy is not inflexible.

At the same time, your organisation will need to consider the property rights of others. You do not want to find that your organisation is liable for infringements by your employees of the property rights of others. Nor do you want to find that your organisation's own ICT has facilitated the breach of someone else's property rights and that your organisation could be implicated in legal proceedings.

Whatever security measures your organisation decides to implement is a matter for determination by the organisation's management. Once management has made those decisions, they should then be communicated in policy documents in a clear and concise way, so that every person affected is made aware of them.

If your organisation is considering implementing security measures that either are, or are potentially, invasive in respect of individual people, then you should seek specialist advice at that time. This is not stated so as to put your organisation "off" the idea, but to ensure that you get current information on any additional obligations this measure may impose on you. This comment applies to any type of surveillance technology (software and hardware) where the collection of personal information is an issue.

## Employment rights

Your organisation has a right to prescribe levels or standards of conduct in respect of people, the workplace, and the tools in the workplace. It is important at the initial stages of drafting your organisation's ICT policies to think about who can be affected by the use or misuse of it, and how they can be affected. This makes it easier to recognise which other policies may need to be considered so that all of your organisation's policies are consistent with one another.

Under this heading, your ICT policies will need to recognise that while employees owe the employer a duty of trust and confidence, the employer has an obligation to provide a safe workplace for all of its employees. Sometimes this means that privacy considerations and employment obligations collide. For example, the use of email to send harmful material around the organisation that targets one person or a group of people in particular could constitute:

- Harassment; and
- Unlawful discrimination (under either the Human Rights Act 1993 or the Employment Relations Act 2000); and
- Misuse or unauthorised use of electronic mail; and
- Misuse or unauthorised use of the employer's time.

While you wouldn't necessarily deal with the conduct under all four headings at the same time, it shows that harassment and unlawful discrimination can occur by electronic means as well as physical or verbal means. And it shows that this conduct usually takes place on the employer's time, at the employer's expense, and using the employer's property.

You will want your policy to clearly establish permitted use of its ICT; while you may have anti-virus protection installed on your network you cannot guarantee that this will prevent the introduction of a virus if people are not instructed to delete, without opening, files that they do not recognise. Further, while it is possible to install disabling devices onto laptop computers, this will not prevent laptop computers, left visible on the seats of parked cars, being stolen.

As a final point, your organisation may want to ensure that in the event of an employee causing it financial loss, that the employee is obliged to indemnify your organisation for that loss. In some circumstances it may be appropriate to consider including provisions authorising deductions (where they are signed by the employee(s) concerned) from salary or wage payments in your organisation's ICT policies; in other circumstances a provision expressing the obligation to indemnify the organisation will be sufficient.

### Enforcing the policy

It is important to ensure that your organisation is sufficiently equipped and prepared to administer the ICT policy. This means that where a particular action is forbidden, for example, forwarding an offensive email, the organisation is able to ascertain whether this has occurred and is prepared to follow the policy in terms of the appropriate outcome, on each occasion. To be effective, the policy must be adhered to and should not be applied inconsistently or differently for different employees.

## Conclusion

Writing ICT policies should not be considered "rocket science". All these policies, as with any other policies, need to reflect is what use is authorised, and what use may constitute misuse and abuse. They need to be realistic, manageable, and enforceable; and they need to compliment or reinforce the organisation's employment agreements, employee handbooks, and disciplinary procedures. They should clearly express the organisation's expectations and how the organisation will monitor those expectations; and should also communicate how breaches of its policies will be handled.

Your policies should reflect a balance between the need to protect the organisation and individuals against the use or misuse of your ICT, and the need to be realistic about personal use of a business resource. They should also recognise that the employment relationship is ongoing and that it can be damaged by an overly restrictive approach to the issues.

A sample policy is not provided as it will vary greatly depending on the specific workplace and other relevant policies already in place therefore an ICT policy will need to be individually tailored. However, EMA does have available a sample clause for Individual Employment Agreements regarding social networking. Additionally, you can contact EMA legal to assist your drafting efforts at a cost. Contact EMA Advice for any advice about, and any assistance with, your ICT policies or for a copy of the sample clause.

## Remember

- **Always call AdviceLine to check you have the latest guide**
- **Never hesitate to ask AdviceLine for help in interpreting and applying this guide to your fact situation.**
- **Use our AdviceLine employment advisors as a sounding board to test your views.**
- **Get one of our consultants to draft an agreement template that's tailor-made for your business.**

This guide is not comprehensive and should not be used as a substitute for professional advice.



Updated: **June 2023**