Example computer, email and internet acceptable use policy

About this document

This document is an example computer, email and internet acceptable use policy for a typical small business.

Usage

This sample agreement has been produced by the IT Donut (www.itdonut.co.uk) and Abussi Ltd (www.abussi.co.uk) to help businesses. It is for illustration purposes only. Seek professional advice when writing your own IT policies.

For more information about creating and implementing IT policies, please visit the IT Donut at www.itdonut.co.uk.

Computer, email and internet acceptable use policy

Effective date: [insert date]
Revision date: [insert date]

To help you do your job, we (<COMPANY NAME>) may give you access to computers, computer files, an email system, and software. You should not password protect any file without authorisation. To make sure that all employees follow this policy, we may monitor computer and email usage. All <COMPANY NAME> email is the property of <COMPANY NAME>.

We try hard to have a workplace that is free of harassment and sensitive to the diversity of our employees. Therefore, we do not allow employees to use computers and email in ways that are disruptive, offensive to others, or harmful to morale.

At <COMPANY NAME> you may not display, download, or email sexually explicit images, messages, or cartoons. You also may not use computers or email for ethnic slurs, racial comments, off-colour jokes, or anything that another person might consider to be harassment or disrespectful.

If you know about any violations to this policy, notify your supervisor, the HR department or any member of management. Employees who violate this policy are subject to disciplinary action, up to and including termination of employment.

<COMPANY NAME> may provide you with internet access to help you do your job. Internet usage is intended for job-related activities but short, occasional personal use is allowed as long as you keep to reasonable limits.

All internet data that is written, sent, or received through our computer systems is part of official <COMPANY NAME> records. That means that we can be legally required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

The equipment, services, and technology that you use to access the internet are the property of <COMPANY NAME>. Therefore, we reserve the right to monitor how you use the internet. We also reserve the right to find and read any data that you write, send, or receive through our online connections or that is stored in our computer systems.

You may not use the internet to write, send, read, or receive data that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.

Examples of unacceptable content include (but are not limited to) sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

If you use the internet in a way that violates the law or <COMPANY NAME> policies, you will be subject to disciplinary action, up to and including termination of employment. You may also be held personally liable for violating this policy.

The following are some examples of prohibited activities that violate this internet policy:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organisation's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorisation
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organisation
- Violating copyright law
- Failing to observe licensing agreements

- Engaging in unauthorised transactions that may incur a cost to the organisation or initiate unwanted internet services and transmissions
- Sending or posting messages or material that could damage the organisation's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organisation or person
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardising the security of the organisation's electronic communications systems
- Passing off personal views as representing those of the organisation
- Sending anonymous email messages
- Engaging in any other illegal activities