#

**Information Communication & Technology (ICT) Usage Policy**

***Overview***

[Company Name] has implemented an Information Communication & Technology (ICT) Usage Policy. The policy takes effect immediately. This policy has been developed to inform employees of our expectations while employed by [Company Name].

[Company Name] sets guidelines and policies in the workplace as follows. We believe it is important to clearly communicate our expectations of all employees. It is every employee’s responsibility to act in accordance with this policy.

***Application***

This policy applies to all employees of [Company Name] regardless of whether they are permanent full-time, permanent part-time or casual employees. The Policy applies to all employees while at any [Company Name] workplace and any other place where the employee performs work for the business.

This policy applies to all employees and clients while they are in a workplace under the management and control of [Company Name] and/ or using computer equipment, communications equipment such as telephones, the internet and/or email.

***Computer, communications devices, e-mail, and Internet usage***

Use of these resources by employees of [Company Name] is permitted and encouraged where such use supports the goals and objectives of the business.

Importantly though, employees must consider and accept that access to the resources provided by [Company Name] is a privilege and all employees must adhere to this policy.

* employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and only personal use during [Delete after reading: amend this point if personal use is prohibited. If personal use is prohibited, this needs to be clearly communicated, as well as advising that usage is monitored] breaks is permitted
* job-related activities include research and educational tasks that may be found via the Internet that would assist in an employee's role
* all Internet data that is composed, transmitted and/or received by [Company Name] computer systems is considered to belong to [Company Name] and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
* the equipment, services and technology used to access the Internet are the property of [Company Name] and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
* emails sent via the company e-mail system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
* all sites and downloads may be monitored and/or blocked by [Company Name] if they are deemed to be harmful and/or not productive to business
* the installation of software on [Company Name] property is strictly prohibited without the express permission of the [Insert Position (e.g. CEO/Director/Owner)].

Unacceptable use of the internet by employees includes, but is not limited to:

* access to sites that contain obscene, hateful, pornographic, unlawful, violent, or otherwise illegal material
* sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via [Company Name] email service
* using computers to perpetrate any form of fraud, and/or software, film, or music piracy
* stealing, using, or disclosing someone else's password
* downloading, copying, or pirating software and electronic files that are copyrighted
* sharing confidential material, trade secrets, or proprietary information outside of the company
* hacking into unauthorized websites
* sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
* introducing malicious software onto the company network and/or jeopardizing the security of the organisation's electronic communications systems
* sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
* passing off personal views as representing those of the company

***Electronic Mail***

Email from a company email address is [Company Name] correspondence and has the same legal implications for both the sender and the Company as correspondence on letterhead and should be treated accordingly.

You and/or [Company Name] may be liable for what is said in an email message and therefore, good judgement, common sense and careful discretion are required. Always seek guidance from your Supervisor if you have any concerns about your email being misunderstood or you are concerned that it may cause a problem.

All electronic email must be sent with a clear identity as to who is sending the message. Employees must not assume another person’s identity or attempt to conceal the origin of the message in any way.

The use of email to send or forward messages which are defamatory, obscene, or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. If any employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, it must not be forwarded to any other address. If this situation does occur, the employee should advise their Supervisor immediately.

It is important to remember that email content that may seem harmless to you may be offensive to someone else. You should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, [Company Name] may consider the response and sensitivities of the recipient of an email, irrespective of the intention of the sender.

***Information (Data)***

Members of staff performing work on company laptops must ensure that such work is backed up on [Company Name] network on a regular basis to ensure all data is captured and protected.

Any employee who is unsure how to back up work on the network should contact the [Insert Position (e.g. CEO/Director/Owner)] for assistance.

Information on the network is [Company Name] property and, in many cases, may be information that is confidential, must be protected and should not be copied or distributed. If an employee needs to copy data for any reason (whether by saving data to a USB stick, emailing data to their personal email account or otherwise) the employee must obtain the [Insert Position (e.g. CEO/Director/Owner)] prior approval. Failure to obtain prior approval is serious and may result in disciplinary action. For more information, employees should refer to the Intellectual Property clauses in their employment contract.

Only software approved by [Company Name] may be installed and utilised on the company’s computers, in accordance with the relevant licence. Staff are not to install software of any nature, under any circumstances. Due to the complex nature of our network, only ICT personnel are to conduct installations to protect the integrity of our infrastructure.

Under no circumstances may company owned software be copied by employees.

Only company owned/provided hardware is to be attached to or used. This is to ensure hardware and software is protected from damage due to viruses or system incompatibility.

Employees who use portable hardware such as laptops, tablets, or mobile phones provided by [Company Name] for business related activities are responsible for the safekeeping, including related passwords or security devices. Any damage, loss or operational failure must be promptly reported to the [Insert Position (e.g. CEO/Director/Owner)].

A firewall restricting electronic access is in place for the protection of the Company’s internal computer networks. Wherever it has been possible to do so, the firewall will restrict ability to visit some web sites and operate certain software programs. Should an employee require access to any item that is restricted, they should speak to the [Insert Position (e.g. CEO/Director/Owner)] in order for access to it to be considered.

***What do I need to do?***

You need to review the Information Communication & Technology Usage Policy and make yourself familiar with the contents of the policy. In the event that you are required to travel, make sure you complete a written request for approval, outlining all details of the trip, by either the [Insert Position (e.g. CEO/Director/Owner)].

***What happens if I do not comply with the Information Communication & Technology Usage Policy?***

The consequences of a breach of this policy will vary depending on the type and seriousness of the breach and will be at the discretion of [Company Name]. The recommendations described in this policy are not intended to be exhaustive, nor do they anticipate every possible use of the Company’s electronic facilities, staff should contact either the [Insert Position (e.g. CEO/Director/Owner)] with any queries relating to appropriate ICT use in the first instance.

Depending on the circumstances, [Company Name] may take disciplinary action up to and including termination of employment.

***Policy and further information***

To the extent that the contents of the Information Communication & Technology Usage Policy refers to obligations on [Company Name], they are guidelines for management or summaries of applicable legislative requirements only and are not contractual terms, conditions or representations on which a staff member may rely.

[Insert Position (e.g. CEO/Director/Owner)] is available to assist with any queries you have relating to the policy which is detailed above.

***Document Control***

This Policy will be reviewed on a regular basis and approved by the [Insert Position (e.g. CEO/Director/Owner)].

|  |  |  |  |
| --- | --- | --- | --- |
| Implementation date | Author | Approved by | Date of next review |
| [Date] | [Name] | [Position] | [Month, Year] |