# Information and Communication Technology Policy (ICT)

## Definition and Scope of Policy

Information and Communication Technology (formerly known as Internet, email and computers policy) defines the boundaries of how <Company Name> employees use Internet, email, computers, phones and other devices at <Company Name>.

The term ICT (information and Communication Technology) is used to describe the communication resources in <Company Name> including computers, servers, networks, wi-fi, phone, email, websites, databases and any other devices that are used for communication in <Company Name>. All employees in <Company Name>, no matter what their role is, will come in contact with <Company Name> ICT and you need to make yourself familiar with the boundaries that exist around its use.

## The bottom line...

***<Company Name> provides its employees with access to informations systems including Internet and email for professional work purposes. We will monitor the use of these resources and take appropriate action if you are found to have abused this service.***

## Responsibilities of <Company Name>

We provide you with access to the Internet and other ICT resources on the basis that you will use it for legitimate <Company Name> business (including job seeking and job related research) only.

<Company Name> will :

- Provide employees with access to ICT equipment requires for work purposes
- Provide access to internet services for the purpose of using <Company Name> on-line services
- Monitor ICT usage to ensure that employees abide by the boundaries of this policy
- <Company Name> will refer the matter to an Garda Siochana if a breach of policy is serious enough and laws have been broken,.

## Responsibilities of Individual

It is the responsibility of the individual to be aware of the regulations and guidelines - Ignorance of these regulations and guidelines is not acceptable as an excuse or defence.

A user should never allow their ID for logging in to be used by other users as all staff must have their own ID which determines which systems they have access.

When your computer is unattended then please log out or lock the session. Prior to this you should customise the power options so that your computer switches to low power or economy mode when not in use.

Users must take adequate precautions to protect the computing resources of <Company Name> from malicious software (e.g. computer virus programs). If you are using your own laptop contact IT Support in <Company Name> for details of which virus protection software to use.

Users have an obligation to make themselves aware of the licensing conditions attaching to software being used by them and to comply with those conditions. Users are reminded that software should not be illegally acquired, copied, used or distributed.

Incidental personal use is permissible provided it does not consume more than a small amount of resources, does not interfere with your productivity, is not for private business activities, does not preclude others with genuine work needs from accessing the facilities and does not involve any illegal or unethical activities.

## Acceptable Usage

To be safe when it comes to the internet and other ICT services, keep your usage strictly work related and remember that the computers, servers, networks etc are <Company Name> property and subject to search and monitoring at all times.

The use of ICT is monitored by our ICT team who administer the network and other ICT services. Your browser history will be checked on a regular basis and there are other technologies available and in use that monitor usage in <Company Name>. We ask you be vigilant to log off your computer (if you have one) and restrict access to it. If you see someone else accessing inappropriate content please inform a manager discretely.

Users of the facilities should exercise extreme caution when using Internet facilities to transmit confidential or sensitive information. IT Support will do its utmost to provide protection against malware but confidentiality cannot be guaranteed with external online web services.

Users of the facilities should be aware of the possibilities that electronic communications might be intercepted, copied, forwarded, printed or stored by others. Particular care should be taken with the transmission of Credit Card details.

Recommended Good Practice for E-mail and Messaging:

- Be concise and to the point.
- Use a meaningful Subject.
- Use good structure and layout.
- Do not use e-mail to discuss confidential information.
- Avoid sending unnecessary attachments.
- Spell check all e-mails prior to transmission.
- Re-read the e-mail before you send it.
- Answer swiftly and only use "Reply All" when really necessary.
- Answer all questions and pre-empt further questions.
- Never reply to spam or junk e-mails nor click on hyperlinks embedded in them - you are merely confirming your existence to the spammers.
- Only request "delivery and read receipts" when certification is essential.
- When replying to mail received as a member of a mailing list, take care to note whether your reply is to the individual sending the message or to the whole list. It is particularly important for users to delete unwanted emails from such mailing lists which can accumulate whenever the user is not in regular touch with office network.

## Inappropriate Usage

<Company Name> emails must only ever be used for professional <Company Name> communication. If you are found to be using the email for inappropriate uses then disciplinary action may be taken.

What kind of actions would be deemed inappropriate?

- Accessing pornographic sites
- Forwarding or generating inappropriate emails
- Accessing websites that incite hatred or promote terrorism
- Using the internet to gamble
- Using the internet to bully, threaten or slander other employees, volunteers or clients of <Company Name>
- Using a <Company Name> email account to send emails that are not related to the business of <Company Name>.
- Misrepresenting <Company Name> using a <Company Name> email address
- Accessing private e-mail accounts during work time for non-work-related-use.
- Installing software on <Company Name> computers without consulting the IT Manager.
- Deleting the history of searches on the internet or disabling the history function on the browser
- Using social networking websites other than necessitated for job research or work purposes
- Any other actions where a law is being broken
- Stealing intellectual property belonging to <Company Name>

This is an example list only and there may be other actions not listed here.

**Important Note**: Users must not jeopardise, in any way, the integrity, performance or reliability of IT Resources within <Company Name>. No attempts must be made to circumvent data protection schemes, to uncover security loopholes, to "hack" into systems or to interfere with the intended operation of the computer resources. It is the responsibility of each individual to report suspicious use that they become aware of while working in <Company Name>.

**or**

**Important Note**:
Users are warned that gaining unauthorised access to data and software programs and/or interfering with data belonging to others are criminal offences under the Criminal Damages Act 1991.

## Consequences of Misuse

The action taken by <Company Name> depends on how serious the issue involved is but you should know that we take the above inappropriate usage is taken quite seriously as it can have implications for the whole organisation.
Most of the actions listed above would result in a final written warning or instant dismissal and in the case of there being illegal actions then an Garda Siochana will be notified.

Main References used by BT for updating this Policy

http://www.dcu.ie/info/regulations/computing.shtml

http://www.accountancyireland.ie/Archive/2008/August-2008/Inappropriate-Computer-Use-Is-your-workplace-protected/

http://www.human-resource-solutions.co.uk/