

Information and Communication Technology (ICT) Acceptable Usage Policy.

Objectives

The objectives of the ETB Internet and Email Policy are to:

- Provide secure and controlled access to the Internet from the Desktop PC
- Ensure the ETB Information Systems are in no way put at risk
- Define statutory responsibilities in relation to National and International legal requirements governing electronic information exchange and commerce
- Define standards of use for Email within the ETB
- Define the course of action to be adopted should there be contravention of the procedures, rules and guidelines outlined in this policy.

Scope

This policy applies to any person authorised to have access to The Education and Training Board's information systems. This includes the ETB's employees, contractors to the Board and consultants engaged by the Board hereafter collectively referred to as employees for the purpose of this policy.

This policy applies to all electronic communications systems provided by The ETB including, but not limited to internet, intranet, e-mail, personal computers and laptops, digital cameras, PDA's (personal digital assistants e.g. Palm) analogue telephones, mobile telephones and fax machines. It is the responsibility of both management and staff of the Board to ensure that all such tools are used in accordance with this policy.

All users are expected to use common sense and to conduct themselves in a manner which is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of the Board under many enactments including, but not limited to the following:

- Employment Equality Acts, 1998 and 2004
- Equal Status Act, 2000
- Data Protection Acts, 1988 & 2003
- Education and Training Board Act 2013
- The Companies Acts 1963 - 2001
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1990

Other documentation that is relevant to this policy includes the Board's policies on:

- Grievance and Discipline
- Dignity and Respect at Work - Equality and Diversity
- Harassment and Sexual Harassment

- Bullying in the workplace

General Computer Usage Regulations and Guidelines

Content

All electronic communications created or received using equipment or services owned or provided by The ETB will be regarded as the property of The ETB.

Security and Passwords

All equipment provided by the Board for use by staff remains the property of The Education and Training Board. Employees must not remove any such equipment (computers, laptops, mobile telephones, etc.) from the Board's premises without prior authorisation from their Manager/CE.

It is the user's responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

Users must not engage in conduct that interferes with other's use of shared computing resources and/or the activities of other users.

Users must not utilise any other person's access rights or attempt to gain access to resources or data for which authorisation has not specifically been granted. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.

No staff member may misrepresent himself / herself as another individual. This includes using another staff member's username and password.

Passwords must remain confidential to each user and must not be relayed to any other person. Each user carries sole responsibility for security access to his/her computer.

Software Ownership

All software which is provided by the Board to an employee is licensed and owned by the Board and may not be downloaded, stored elsewhere or transferred to another individual by any employee of the Board.

Under no circumstances should software be downloaded from the Internet or installed from any other source and used on the Board's machines without the prior permission of the Manager/CE. Any breach of these requirements may result in disciplinary action

Confidentiality

When a user registers with a site or a service in the name of the Board the resulting spamming of information may tie up the communications system. Users must not register with an electronic service over the website without prior permission from their

Manager/CE, to avoid the release of confidential Board information to third parties and to avoid interference with the communications systems.

Users must maintain confidentiality while carrying out their duties and while on ETB business.

Privacy

It should be understood that the Board does not provide users with a guarantee or to the right to privacy or confidentiality in connection with the use of any technology and users should have no expectation of privacy in the use of the Board's IT resources.

Monitoring Policy

The ETB reserves the right and intent to monitor e-mail content and Internet usage to ensure technology is being used properly and to protect the Board and its employees from liability under equality, data protection, pornography and copyright legislation. This does not constitute infringement of any individual rights to personal privacy under the Data Protection Acts 1988 and 2003.

Monitoring is carried out on a message size virus protection, correct file attachments extensions, access to external system (including web/internet sites) this list is not exhaustive. Monitoring developments may change over time. In addition the Board will monitor all PC's for inappropriate image and content.

Legal Implications of Storing Electronic Data

All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include but are not exclusive to Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation.

All data must be stored in an up-to-date format. Personal information may contain only information relevant to the individual and to the purpose for which it is being stored. Data must not be used for any other purpose. This data must be maintained in an accurate format and must be altered if the user/Board becomes aware of inaccuracies.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Employees should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by the employer and / or disclosed to third parties.

Material of obscene or offensive nature

Users are subject to all legislation regulating the use of the Board's IT/Communications resources. Users must not store, download, upload, circulate or otherwise distribute material containing:

- a) Any derogatory comment regarding gender, material status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.
- b) Any material of a pornographic nature.
- c) Any material of a paedophilic nature.
- d) Material containing offensive or foul language.
- e) Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail or other computer sources the employee should:

- a) Bring it to the attention of their Manager/CE/HR Manager;
- b) Inform the sender that such images are offensive and that they should refrain from sending such images in future; and
- c) Delete the message.

Virus Protection

Viruses can enter an organisation a number of different ways:

- (a) Un-scanned digital storage media (e.g. CDs, DVDs, floppy disks, USB memory sticks) being brought into the organisation.
- (b) E-mails or attachments
- (c) Downloaded data from the Internet.

Individuals using electronic information must be familiar with and comply with the Board's procedures governing usage of floppy discs, cds and other software.

No computer user may interfere with or disable the Anti-Virus software installed on their desktop PC.

E-Mail

Many employees have a personalised e-mail account to facilitate the sending and receiving of business messages between staff and between the Board and its clients and suppliers. While email brings many benefits to the ETB in terms of its communications internally and externally, it also brings risks to the organisation, particularly where employees use it outside of their The ETB roles.

Every employee has a responsibility to maintain the Board's image, to use electronic resources in a productive manner and to avoid placing the Board at risk for legal liability based on their use. It should be remembered that the contents of e-mail are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act, Data Protection Acts.

Risks Associated with E-Mails

- (a) Messages can carry viruses that may be seriously damaging to the ETB's systems.
- (b) Letters, files and other documents attached to mails may belong to others and there may be copyright implications in sending or receiving them without permission.
- (c) It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching the Board's security and confidentiality.
- (d) E-mail is speedy and, as such, messages written in haste or written carelessly are sent simultaneously and without the opportunity to check or rephrase. This could give rise to legal liability on the part of the Board.
- (e) An e-mail message may legally bind the Board contractually in certain instances without the proper authority being obtained internally.
- (f) E-mails should be regarded as potentially public information which carry a heightened risk of legal liability for the sender, the recipient and the organisations for whom they work.

Rules for E-Mail Use

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly any written, stored or forwarded and disseminated information must adhere to the guidelines within the Data Protection and the Employment Equality legislation and in accordance with the equality policy of the Board.

In order to avoid or reduce the risks inherent in the use of e-mail within the Board, the following rules will be implemented:

- (a) The following text will appear at the end of every e-mail sent from your Board address to an external address. This will be inserted automatically by the e-mail system:

The information transmitted in this e-mail is intended for the addressee only and may contain confidential and/or privileged material. Any review, retransmission, dissemination, reliance upon or other use of this information by persons or entities other than the addressee are prohibited. Opinions expressed in this e-mail may be personal to the author and are not necessarily the opinions of the ETB, if you received this in error, please contact the sender and delete this material.

- (b) The Boards' name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation. Therefore, e-mail messages must be appropriate and professional.

- All Email is to be written in accordance with the standards of any other written communication, the content and language used must be consistent with ETB best practice and each message must be carefully addressed to ensure that they reach the target recipient.
- (c) Correct spelling and punctuation should be maintained in all communications.
- (d) E-mail is provided for business purposes.
- (e) Occasional and reasonable personal use of e-mail is permitted provided that this does not interfere with the performance, work duties, responsibilities and customer service of the Board, does not support any business other than the Board and otherwise complies with this policy.
- (f) An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden.
- (g) E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.
- (h) E-Mails must not contain any inappropriate or lewd content or content likely to cause offence to individuals.
- (i) Distribution lists may only be used in connection with Board business.
- (j) Particular care should be taken when sending confidential or commercially sensitive information. If in doubt please consult your manager.
- (k) Great care should also be taken when attaching documents as the ease with which employees can download files from the Internet or 'cut and paste' materials from electronic sources increases the risks of infringement of the rights of others particularly to copyright, intellectual property and other proprietary rights.
- (l) Where important, you should obtain confirmation that the intended recipient(s) have received your e-mail.
- (m) Documents prepared internally for the public or for clients may be attached via the e-mail. However, excerpts from reports other than our own, may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt consult your manager.
- (n) Do not subscribe to electronic services or other contracts on behalf of the Board unless you have express Board to do so.
- (o) If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your manager or the HR manager.
- (p) It is specifically prohibited to use the Email system for storage, distribution of unsavoury materials, indecent, obscene, pornographic or libellous material.

- (q) Chain mails or unsuitable information must not be forwarded internally or externally.
- (r) The Board reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.
- (s) Notwithstanding the Board's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior written approval from the employer. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message.
- (t) Information Security must authorise distribution of advertisements, mail shots or product material via external mail in advance.
- (u) If you receive unintended Email it is vital that you alert the sender by reply. Should the Email contain confidential or sensitive information, you must not disclose this information to any other Group or individual
- (v) All attachments received should only be opened when employees have first checked the authenticity of the sender and validity of the attachment. All other attachments should be deleted or referred for clearance.
- (w) Should Email received by you contravene ETB Policy - you should inform your Manager immediately.

The Internet/Intranet

Access to the Internet / intranet is provided to staff as necessary solely for the purpose of conducting the Board's business.

Rules for Internet use

- (a) The Board's Internet connections are intended for activities that either support the Board's business or the professional development of employees. During working hours staff should minimise web surfing that is unrelated to these activities.
- (b) General Internet access will only be provided to authorised personnel. Authorised personnel will have responsibility for Internet access under their account and hence will also have responsibility for illicit use of their account with or without their consent.
- (c) Internet usage is monitored on a systematic basis and as deemed necessary by the Board.
- (d) To prevent viruses from being transmitted through the system unauthorised downloading of any software programmes or other material is forbidden.
- (e) Internet use is not permitted for personal gain or profit or to represent yourself as someone else.
- (f) It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the grounds of gender, marital status, family status, age, race,

religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising there from.

- (g) It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material.
- (h) If an employee is downloading pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment by offended parties. Such incidents should be reported to the relevant Board. Apart from any potential offence caused and the inappropriateness of such activity, the Board may be vicariously liable for any claims arising from such behaviour.
- (i) Because of the serious criminal implications of accessing child pornography, any employee found to be accessing such information may be summarily dismissed and the matter referred to An Garda Síochána. Furthermore, should an employee be prosecuted under the Child Trafficking and Pornography Act, 1998, by engaging in such activities outside the remit of the workplace, the Board may find it fitting to invoke disciplinary action.
- (j) The Internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.
- (k) The Internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.
- (l) Public messaging systems on the Internet must not be used by staff save with the prior written permission of a Manager. Public messaging systems include user groups, chat rooms, special interest forums bulletin boards and mobile phone texting sites.

Laptops and Remote Computers

The rules applying to use of the internet and e-mail messaging systems apply also to any laptops, remote computers or other electronic processors in use by the staff member and supplied by the local Board. Express permission must be obtained from the CE or relevant Manager to remove such equipment from the Board premises. All such equipment will be subject to the same monitoring procedure as that which is retained on-site.

Telephone Usage

Access to telephones is intended for Board purposes only. While reasonable making and taking personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. The Board reserves the right to monitor the use of the telephone system.

Some mobile phones are provided to staff members for Board business. Personal calls from such phones are permitted but the calls must be paid for by the staff member. Where such personal calls are necessary staff should seek to use an analogue telephone

where possible. For more specific information see The ETB's Mobile Phones Acquisition and Usage Policy.

During office hours taking and/or making calls on personal mobiles is not strictly prohibited, however, staff are encouraged to keep such calls to a minimum.

Other Electronic Tools

Other electronic equipment (e.g. fax machines, photocopiers etc.) remain the property of the ETB and as such must be treated with care and used only for ETB purposes. Abuse of equipment for personal use or gain may result in use of the disciplinary procedures and in disciplinary action.

Removable Media

No removable media such as CD, DVD, USB drive or floppy disc that contain data or files may be used without first obtaining advice from IT support.

Infringements of Policy

Failure to comply with the policy and guidelines outlined above may result in:

- The withdrawal of e-mail and Internet facilities from the Section, Staff or members involved;
- Initiation of disciplinary procedures and disciplinary action, up and to including dismissal.
- Serious breaches of the policy may result in initiation of criminal or civil proceedings.

Policy Enforcement

Users should report any suspected abuse of computer and network resources, or any unpleasant material or e-mail that may come to their attention as well as any suspected damage or problems with files.

Users, when requested, are expected to co-operate with system administrators and/or other authorised staff in any investigation of system abuse.

Tipperary ETB reserves the right to examine any files-held on its computer systems.

Any user found in breach of this policy shall be liable for legal and Tipperary ETB disciplinary procedures.

This policy is subject to regular review and will be updated when revisions are necessary.