

INTERNET ACCEPTABLE USE POLICY

TABLE OF CONTENTS

Purpose	2
User Responsibilities	2
Acceptable Use	2
Unacceptable Use	3
Privacy Guidelines	4
Security	5
Operational Guidelines	6
Compliance	6
Related Policies and Links	6
Revision History	7

Purpose

The purpose of this policy is to ensure the proper use of the Internet, intranets, extranets, the Web and Internet applications (the "Internet") by **KCETB** "users". Usage of these resources is a privilege that is extended to, but not limited to **employees (both full and part time), students and learners, contractors, Interns, Work Placement Participants, partners and / or consultants**, to be referred to as "Users". This policy applies to any use of the Internet from any corporate network(s) or computing devices, including mobile devices, provided by **KCETB**. It also applies to a user's personal use of the Internet, as directed below.

The Internet is constantly evolving in application and content; this policy is not intended to list all forms of acceptable and unacceptable use. Employees have the responsibility to use the Internet in an efficient, effective, ethical and lawful manner. Internet users must follow the same code of conduct expected in any other form of written or face-to-face business communication.

KCETB may supplement or modify this policy for users in certain roles. This policy for Internet Usage complements similar **KCETB** policies, such as the Technology Acceptable Usage policy. A comprehensive list of ICT policies may be located in the ICT Policy Framework.

This policy applies to all users of "Internet" resources owned or managed by **KCETB**. Individuals covered by the policy include **employees (both full and part time), students and learners, contractors, Interns, Work Placement Participants, partners and / or consultants, external individuals and organisations** utilising "Internet" resources facilitated by **KCETB's** computing facilities.

User Responsibilities

Acceptable Use

- The provision of network access and applications (that is, browsers) to access the Internet is primarily for business-related purposes.
- A discretionary level of personal use of the Internet / internet-based applications is permitted once same is reasonable and does not constitute unacceptable use (see below) and does not interfere with other business activities or employees' work responsibilities. Personal use of the Internet and corporate infrastructure is a privilege, not a right. It may be revoked at any time.
- Using the Internet for personal shopping and personal banking is acceptable, provided it complies with other acceptable-use provisions.
- The Internet provides a plethora of communication mechanisms. All written communication posted to the Internet should strive for the highest level of professionalism, politeness and courtesy. Electronic communication is frequently inadequate in conveying mood and context; therefore, the user should carefully consider how the recipient might interpret a message before composing or sending the message.
- Access to the Internet and Internet application is acceptable only through corporate-issued applications, such as browsers, IM clients and other tools. Non-sanctioned applications must be approved by **KCETB's ICT Services Team** following the normal approval process.
- Use of the Internet may expose employees to offensive content and/or criminal activity. **KCETB** accepts no liability for employees' non-business-related activity on the Internet.

Unacceptable Use

The following is a list of actions or activities that would generally constitute unacceptable use. (**Note:** This list is intended to be a guideline for users when considering what is unacceptable use and is not comprehensive.)

- Accessing Web sites or applications that contain content that can be reasonably interpreted as offensive, harassing, obscene, promoting violence or hate, racist, sexist, ageist, gambling, adult or pornographic, or sites that deal with criminal activity, including (but not limited to) those involving or related to illegal drugs, computer hacking/cracking, the creation of malicious software (malware), terrorism, and illegal weapons.
- Using search terms that are likely to result in lists of, or images from, unacceptable Web sites (as defined above).
- Accessing Web sites or applications for personal use that consume excessive network resources for long periods of time, such as multiplayer games, virtual worlds, large file transfers and streaming media.
- Internet use that interferes with the employee's work duties and responsibilities
- Unauthorised use of copyrighted material from the Internet, such as downloading copyrighted music or movie content via peer-to-peer (P2P) networks.
- Using software or Web sites (often called "anonymisers") that attempt to hide Internet activity for the purpose of evading corporate monitoring.
- Operating a business or any undertaking that offers personal gain or benefit
- Downloading of computer utilities or tools that are primarily designed for gaining illegal access to other computer systems (usually referred to as hacking or cracking tools).
- Unauthorised attempts to break into, or illegally access or damage, other computer systems or data. (Note: **KCETB** is not responsible for an employee's use of the Internet that breaks laws.)
- Forwarding corporate e-mail messages to personal e-mail accounts, because of unacceptable risks associated with privacy, security and compliance.
- Any **KCETB** email address must not be used for any internet subscription, unless there is an underlying business rationale.
 - Should further clarification be required, contact your line manager
- Harassing other users on the Internet or interfering in another user's work or use of the Internet. This includes, but is not limited to, the sending of unwanted e-mail, IM or chat messages.
- Publishing, downloading or transmitting content or messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.
- Creating, exchanging, publishing or otherwise distributing in public forums and open communication tools to third parties (for example, via Web e-mail, IM, blog postings, chat rooms, Twitter, virtual representatives and more) any of the following:
 - 1 Product advertisements
 - 2 Political lobbying
 - 3 Religious promotion.
- **KCETB** confidential information to unauthorised persons or violating **KCETB's data protection and GDPR policy**.

- Otherwise using the Internet in a way that increases **KCETB's** vicarious, legal or regulatory liability.

Any security issues discovered will be reported to the head of ICT or their designee for follow-up investigation. Additional reporting requirements can be located within the Compliance section of this policy.

Privacy Guidelines

Users should have no expectation of privacy. **KCETB** maintains the right to monitor and review user(s) Internet activity to ensure compliance with this policy, as well as to fulfil **KCETB's** responsibilities under the laws and regulations of the jurisdictions in which it operates.

- **KCETB** reserves the right to intercept, monitor, record, review and/or disclose any and all user Internet sessions. Monitoring may be performed with the assistance of URL filtering and/or content-filtering and or monitoring software, or by designated **KCETB** employees and/or designated external entities.

Monitoring may be performed by automated software and logs, and alerts would be sent to the ICT Services Team and / or designated staff members.

Requests to monitor/review internet activity can be submitted to the KCETB ICT services team by head of centres/departments, KCETB Directors or the Chief Executive. The ICT Services team will initiate a review of internet activity based on this request subject to the appropriate level of approval from management.

In their role on the ICT Services Team, ICT staff may come into contact with data that may identify an individual user's internet activity.

If the ICT Services Team or designated staff members at any stage identify un-acceptable internet activity, this will be reported to the appropriate member of management. This can include Heads of Centres/Departments, KCETB Directors or the Chief Executive.

- **KCETB** reserves the right to alter, modify, reroute or block Internet sessions, as appropriate. This includes, but is not limited to:
 - 1 Rejecting, quarantining, or removing attachments and/or malicious code from Web pages or FTP file sessions that may pose a threat to **KCETB's** resources
 - 2 Blocking downloadable files and long-lived content, such as music, movies and gaming sessions, that are considered to be of little business value and that involve a significant resource cost
 - 3 Rerouting content found in Internet messages or posts (for example, via Web e-mail, IM, blog postings, chat and Twitter) with suspicious content to designated **KCETB** employees for manual review
- Electronic messages and internet / intranet activity are legally discoverable and permissible as evidence in a court of law
- Any evidence of suspected or alleged illegal activity discovered during monitoring or reviews will be dealt with through **KCETB's** disciplinary procedure and may lead to a further criminal investigation. Refer to **KCETB's** relevant disciplinary policy for further information

Security

As with any type of software that runs over a network, Internet users have the responsibility to follow sound security practices:

- The Internet is the No. 1 transmission vector for malware and viruses. Please exercise extreme caution when surfing the Internet. Even well-respected, branded sites may host malicious content, or may link to sites that do. A good rule of thumb is to be wary of unexpected pop-up windows requesting your permission to take some action (such as download additional browser components). If a Web site is behaving strangely, then close your browser and notify **KCETB's ICT Services Team**.
- Downloading free or "demo" software via the Internet from unknown providers may cause unnecessary security risks, support issues and/or legal liability. If you require software for a specific business purpose, including for evaluation and testing, then please contact **KCETB's ICT Services Team**.
- Do not click directly on hyperlinks in e-mail, unless it is an expected communication from a known and trusted source. Normal procedure to get to a site, is to open a browser and type the address in the browser address bar. If you do not know the exact addresses, then go to the primary site and use the site navigation to get to the exact page.
- Internet users should not post to any Web site, or use any Internet communications services, to transfer or distribute sensitive data, such as user names, passwords, PPS numbers or account numbers, over the Internet without appropriate controls, such as encryption, except in accordance with **KCETB's data protection policies**. Sensitive data passed over the Internet could be read by parties other than the intended recipients, particularly if it is clear text traffic. Malicious third parties could potentially intercept and manipulate Internet traffic.
- Attempts to circumvent this policy through the use of anonymous proxies, software or hardware will be considered a violation of the policy.
- **Do not share your network account password** or allow another person to use your account. Do not use another individual's account.
- Do not store corporate information in public storage services unless they are sanctioned by KCETB's ICT Services Team.
- Do not use Peer to Peer file sharing networks.
- Do not use remote access tools (for example, Go to My PC, TeamViewer, LogMeIn or remote desktop) unless they are supplied and sanctioned by **KCETB's ICT Services Team**.
 - Should further clarification be required, contact your line manager or **KCETB's ICT Services Team**
- E-mail, IM and other message attachments can contain viruses and other malware. Users should only open attachments from known and trusted correspondents. KCETB's ICT Services Team should be notified immediately if a suspicious email / attachment is received.
- Users will not be directed (via e-mail, from **KCETB's ICT Services Team** or from any other entity under **KCETB's** remit) to sites requesting personal information, such as usernames or passwords. Such requests should be forwarded to KCETB's ICT Services Team. Such approaches — known as phishing — are fraudulent and carried out for purposes of unlawful exploitation.
- Users are cautioned to only use trusted networks to access the Internet from corporate devices while out of the office. Do not use open consumer wireless (Wi-Fi) networks. Do not attempt to bridge networks or modify firewall settings.

Operational Guidelines

KCETB employs certain practices and procedures to maintain the health and efficiency of resources, to achieve **KCETB's** objectives and/or to meet various regulations. These practices and procedures are subject to change, as appropriate or as required under the circumstances.

The following guidelines apply to any KCETB device or any device used to access the internet through KCETB networks:

- Devices must contain up to date anti-virus software.
- Devices must be configured with an operational firewall
- Devices must be kept up to date with OS patches and hot-fixes
- When browsing the internet, devices must use one of the following web-browsers unless specific authorization is received from the KCETB ICT Services Team
 - Microsoft Edge
 - Microsoft Internet Explorer
 - Mozilla Firefox
 - Google Chrome
 - Apple Safari
 - Opera
- Devices must not be configured to access the internet via TOR or similar software/services

Compliance




Individuals found to be in breach of this Internet Acceptable Use Policy, may be subject to disciplinary action, up to and including dismissal. For further information, refer to **KCETB's** disciplinary policy.

For the avoidance of doubt, where questions remain as to what constitutes “appropriate use”, contact **KCETB's ICT Services Team** for full clarification.

Related Policies and Links

KCETB Disciplinary Policy
KCETB Data Protection Policy
KCETB Data Retention Policy
KCETB Email Usage Policy

Authority and Ownership

OWNER	TITLE	DATE	SIGNATURE
Enda Curran	IT Administrator	17/01/2020	
Colin Hamilton	IT Administrator	17/01/2020	
AUTHORISED BY	TITLE	DATE	SIGNATURE
Liam Scott	Director of OSD	17/01/2020	

Revision History

VERSION	DESCRIPTION	REVISION DATE	REVIEW DATE	APPROVER NAME
1.0	INITIAL VERSION	17/01/2020	30/06/2020	Liam Scott