KTCEA Administrative Procedure 656
Updated: September 1, 2022

Network and Data Security

Background

KTCEA is a strong advocate of using technology to support teaching and learning, and recognizes that digital literacy is a crucial skill set for students and staff to develop. In addition, KTCEA is dependent on its technology systems to maintain key student records and to support its major operations and administrative functions. As a result, KTCEA generates and stores large amounts of data, much of which is sensitive, private or confidential. Keeping this data secure is a priority for KTCEA, and is fundamental to protecting systems from outside attack and preventing personal information from being stolen and used to harm people or families.

Guidelines

KTCEA believes that all stakeholders, including families, students, and staff, have roles to play in maintaining the security of digital information.
Data security is particularly important when transferring and storing information on the network or on cloud-based services.
KTCEA is committed to developing training programs that educate users in the area of data security, and it is expected that users will actively support the broad goal of keeping KTCEA data secure.

#	Procedure	Roles & Responsibilities
1.	Establish, administer and implement network security guidelines and procedures, and update them as required.	IT Manager
2.	Develop an organization-wide training program and associated training materials for staff and students, and ensure that all staff are trained in data security on an ongoing basis or as part of an on-boarding process for new staff.	IT Manager, HR Manager
3.	Establish, install and implement data backup and recovery systems for all KTCEA servers and devices.	IT Manager
4.	Acquire and install anti-virus software on all KTCEA technology systems and devices.	IT Manager
5.	Provide guidance and direction for network security and authorize protocol changes in emergency situations, such as a virus attack or other data breach.	IT Manager
6.	Ensure that all obsolete, end of support, surplus IT equipment has been decommissioned.	IT Manager
7.	The IT Manager or designate shall install software and other applications on KTCEA systems and devices; conversely, no staff-person or student other than the IT Manager or designate	IT Manager or Designate

	shall install software or other applications on KTCEA hardware or devices.	
8.	The IT Manager or designate shall exclusively manage and control the operation of the KTCEA network and wireless network entry points, including security/encryption protocols; conversely, no staff-person shall connect any device to the KTCEA network service, such as a personal web server, File Transfer Protocol (FTP) server, news server, electronic bulletin board, RSS feed, local area network or modem connection.	IT Manager or Designate
9.	Users may only use cloud-based applications or storage when 9.1 the privacy agreement with the cloud-based service provider contains clauses that compel the provider to adhere to the Freedom of Information and Protection of Privacy Act. 9.2 the service is hosted on a country where legislation does not allow the potential to override the Freedom of Information and Protection of Privacy Act. 9.3 any data accessed or transferred is encrypted and password protected.	IT Manager, Users
10	The Superintendent or designate will approve all Vendor Privacy Agreements.	Superintendent
11.	All staff will report any breach of information security, whether actual or suspected, to their direct supervisor who in turn will report it to the IT Manager for review and remediation.	All Staff, IT Manager
12.	All users have a responsibility to ensure the overall security of KTCEA data in accordance with this Administrative Procedure, AP 140A Responsible Use of Technology – Students, and AP 140B Responsible Use of Technology – Staff.	Students, Staff and Stakeholders
13.	Breach of any provision of this Administrative Procedure is deemed to be a misuse of technology as set out in AP 140A Responsible Use of Technology – Students, and AP 140B Responsible Use of Technology – Staff, and is subject to any associated disciplinary action as prescribed.	Students, Staff and Stakeholders

Definitions:

Technology means “KTCEA-owned electronic equipment, communications network and servers, devices and systems, email and social media accounts, digital programs and associated applications that are owned or licensed by KTCEA including any data and content therein, as well as any personal electronic equipment, devices or social media platforms that are used on or near KTCEA schools and facilities or on school days.”

Social media refers to “electronic access to and use of blogs, personal websites, RSS feeds, postings on wikis, micro-blogs, podcasts and other interactive sites, such as, but not limited to: Facebook, YouTube, Instagram, Blogger, Twitter, Instant Messaging, and postings on video or picture-sharing sites and elsewhere on the internet.”

References:

Policy 3 – Respectful, Caring and Safe Schools and Workplaces
Policy 13 – Technology and Student Information
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
AP 140A Responsible Use of Technology - Students
AP 140B Responsible Use of Technology - Staff
AP 140C Digital Citizenship Agreement for Responsible Use of KTCEA Technology

Procedure Amendments and Updates

The responsibility for updating and amending this procedure rests with the Associate Superintendent Facilities & Operations.