CAPE-Centre for Academic and Personal Excellence
Policy Manual

Policy 2.15
Category: Governance and Operations

Electronic/Internet Security

BACKGROUND

Technology is an integral aspect of the program at CAPE. It enhances the global learning experience of the students and is a means of achieving efficient and effective program delivery, enhancement, and assessment. Expedient sharing of relevant information with and among students, colleagues, parents, and community is part of the everyday life at CAPE. Therefore, CAPE believes that access to current technologies is crucial to the educational program. However, security issues must be addressed to ensure that private and/or sensitive information is protected, and that individuals are protected against unwanted, unsolicited communications.

POLICY STATEMENT

The CAPE Charter Board believes in the role that technology plays in the delivery, enhancement, and assessment of the CAPE educational program and in the expedient sharing of information that technology provides. The CAPE Charter Board also believes that appropriate security measures are absolutely necessary to safeguard private information and protect all CAPE technology users against unwanted, unsolicited communications and/or access to undesirable sites. The CAPE Charter Board is also committed to safeguarding the privacy of all its stakeholders, students, parents, staff and community by securing all private information that is on site.

DEFINITIONS

1. **Security -** protection resulting from all measures designed to deny unauthorized persons information of value or personal private information or of sensitive nature.
2. **Technology -** methods, systems, and devices which are the result of scientific knowledge being used for practical purposes.
3. **Protocol -** a system of rules that explain the correct conduct and procedures to be followed in formal situations.
4. **Password -** a string of characters used to verify the identity of a user during the authentication process.
5. **Access code -** a series of numbers and/or letters that allow access to a particular system.

Policy 2.15
Category: Governance and Operations

GUIDELINES

6. **On-site Physical/Hard Copy Security:**

6.1 The CAPE Charter Board encourages and supports on-site physical security measures that safeguard private information and facilitates safe usage for all users.

6.2. The Superintendent is responsible for the structuring of protocols for securing hard copy sensitive and private information.

6.3 The School-based Administration is responsible for ensuring that the security protocols are shared with all staff and followed at all times.

6.4 These security protocols are to be reviewed annually.

6.5 Access to sensitive and private hard-copy information must be granted on need-to-know basis only by the Superintendent or the principal, as required by the duties to be discharged by the employee.

6.6 Each staff member is bound by FOIP, *Alberta Education Code of Professional Conduct: Charter School Teachers* and CAPE's Codes of Conduct when in possession of any sensitive and private information.

7. **Electronic/Internet Security:**

7.1 The CAPE Charter Board encourages and supports on-site electronic internet security measures that safeguard private information and facilitates safe internet usage for all technology users.

7.2 The CAPE Charter Board researches, or causes to be researched, available security packages and approves all security measures prior to use in the school and supports on-site electronic/internet security measures that safeguard private information and facilitates safe internet usage for all technology users.

7.3 The Superintendent is responsible for the structuring of protocols for securing electronic sensitive and private information.

7.4 The School-based Administration is responsible for ensuring that the security protocols are shared with all staff and followed at all times.

7.5 These security protocols are to be reviewed routinely but especially when new technologies are introduced.

7.6 The Superintendent is responsible for ensuring that the CAPE Network is secure, that internet access is restricted and monitored, that personal devices are secured through passwords and access codes, and that all necessary measures are taken to ensure responsible and safe technology utilization.

7.7 The School-based Administration is responsible for ensuring that all security measures are followed by all CAPE technology users.

7.8 Access to sensitive and private electronic information must be granted on a need-to-know basis only, as required by the duties to be discharged by the employee.

7.9 Each staff member is bound by FOIP, the profession's Code of Conduct and CAPE's Codes of Conduct when in possession of any sensitive and private information.

References:

Freedom of Information and Protection of Privacy Act
CAPE charter 2020
Education Act
CAPE Code of Professional Conduct for Certificated Staff
CAPE Code of Professional Conduct for Non-Certificated Staff
ATA Code of Professional Conduct
Alberta Education Code of Professional Conduct: Charter School Teachers

---

Adopted: March 22, 2012 Motion: #2012-5-22-8
Reviewed: April 2013
Reviewed: August 2018
Reviewed: October 2021