



Windsor-Essex Catholic District School Board

Section: **Human Resources**

Policy: **Employees' Acceptable Use of Electronic Access, Information Technology & Data**

H:17

POLICY

The clear expectations of the Windsor-Essex Catholic District School Board with respect to the acceptable use of information technology equipment, electronic access and data owned by the board are outlined below:

Appropriate Use

Information technology equipment and data owned by the Board are to be used solely for the furtherance of the Board's objectives and for an educational purpose. The term *educational purpose* encompasses classroom activities, professional and career development and administrative services that support education. *Educational purpose* does not include:

- Commercial Use – employees may not use the Board's system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use.
- Political Lobbying – employees may not use the Board's system for political lobbying.

Use by other external individuals or organizations is prohibited unless specific prior approval is obtained.

Electronic mail originating from the Board, like traditional mail, is to be used only to further the Board's objectives, and is the Board's property. As part of regular, day-to-day business operations, the Board DOES NOT monitor internal mail and communications. Should a specific need arise, the Director can, in consultation with the Chairperson of the Board, request that specific electronic mail and communications be monitored.

Illegal Use

Information technology equipment and data owned by the Board are not to be used for illegal purposes. Employees will not:

- Attempt to gain unauthorized access to the Board's system or to any other computer system through the Board's system, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files. These actions are illegal, even if only for the purposes of browsing.
- Have in their possession, or install on any computer a password cracker, keystroke logger, network

sniffer or any other utility that can be used to “hack”, unless specifically authorized by the Board. The Board recognizes the extent of the threat posed by computer hacking and has zero tolerance for this behaviour.

- Make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal and will be dealt with as such.
- Use the Board’s system to engage in any other illegal act, such as arranging for the sale or purchase of restricted substances such as alcohol and drugs, engaging in criminal activity or threatening the safety of a person.
- Use the Board’s system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
- Use the Board’s system to harass or defame another individual.

System Security

It is the active responsibility of each employee to maintain a secure information access environment. Employees will:

- Be responsible for the use of their individual account and should take reasonable precautions to prevent others from being able to use their account. Under no conditions should an employee provide their password to another person.
- Immediately notify a system administrator if they have identified a possible security problem. Most employees are not authorized to deal with security problems; actions may be construed as an illegal attempt to gain access.
- Avoid the inadvertent spread of computer viruses by following the Board’s virus protection procedures.
- Adhere to the requirements set out in the “Agreement for Authorized Windsor-Essex Catholic District School Board Staff for Notebook Computers”, ensuring that live updates are run daily for both anti-virus software and operating system’s security updates. No laptop shall be connected to the Board’s network until it has been checked for compliance by an IT technician. Periodic verification of adherence to this Board policy will be performed randomly by a software support technician.
- Connecting personal laptops to the WECDSD network is strictly prohibited. Specific permission by the IT Department is required to use a personal laptop on the Board’s network and that laptop must adhere to expectations concerning anti-virus, security updates, and restricted software as outlined

in this policy. If permission is granted, the identified personal laptop must be registered with the school support technician prior to connecting to the Board network.

- Not add ANY additional components to the Board's network environment – such as, but not limited to – modems, wireless access points, routers, hubs. If additional components are needed, they must be specifically approved and installed by an IT technician.

Inappropriate Language

Restrictions against inappropriate language apply to public messages, private messages and material posted on Web pages. Employees will not:

- Use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, racist or disrespectful language.
- Post information that, if acted upon, could cause damage or a danger of disruption.
- Engage in personal attacks, including prejudicial, discriminatory or slanderous attacks.
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If an employee is told by a person to stop sending him/her messages, he/she must stop.
- Knowingly or recklessly post false or defamatory information about a person or organization.

Respect for Resource Limits

Electronic access time and data storage space are limited resources. To best utilize these resources, employees will:

- Not post chain letters or engage in spamming. Spamming is sending an annoying or unnecessary message to a large number of people.
- Avoid downloading large amounts of material. If it becomes necessary to download a large file, employees will do so at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer.
- Check their e-mail frequently and delete unwanted messages promptly. Disk quotas are imposed on e-mail accounts; exceeding the quota will block additional incoming mail for that account until the mailbox is brought below quota.
- Adhere to the guidelines as published periodically for use of the First Class bulletin board.

Copyright Infringement and Licensing

Employees will respect the rights of copyright owners, including software manufacturers. All software resident on the Board's computers must be installed in compliance with licensing requirements of the software's owners. Use of 'pirated' or software secured through unauthorized reproduction is strictly prohibited. Individuals may be held liable in the event that software is not licensed or properly authorized.

Respect for Privacy

The Board recognizes and respects its disclosure and privacy protection obligations as identified in *The Municipal Freedom of Information and Protection of Privacy Act*. Additionally, the *Ontario Student Record Guideline, 1989, Section 4* requires that all staff will strictly observe secrecy with respect to pupil-identifying records, including health and other records, maintained by the Board.

- Employees will respect the Board's obligations under the provisions of these regulations.
- Employees using the Board's information are responsible for using it for purposes intended, and complying with control and disclosure procedures.
- Access to personal or confidential information is restricted to those with a demonstrated 'need to know' to the extent required to perform job functions.
- Information and equipment disposal practices ensure the continued protection of privacy.

Information Resources Management and Data Security

The Board's information is a corporate resource with substantial value that must be protected from unauthorized modification, destruction or disclosure, whether intentional or inadvertent.

- Critical data are securely managed throughout the life cycle and backed up as appropriate.
- Software and related intellectual property developed by employees in the performance of their duties are the property of the Board, and may not be distributed or shared unless authorized in writing by the Director of Education or designate.
- Passwords and related security codes must be kept private and protected from inadvertent disclosure. Password owners are responsible for immediately reporting the loss or inadvertent disclosure of a password to the supervisors.
- Where an application allows the setting of an administrative password or security code, that password may be requested by IT. The employee must maintain a secured list of the applications or databases, along with the assigned passwords or security codes, and submit this list annually or

upon changes, to the IT department where it will be stored securely.

- Data, computer equipment and software must be protected at all times from physical damage, theft or unauthorized modification by those responsible for its use and physical security.
- Primary responsibility for security of information is vested with the supervisory Officer responsible for the creation or assembly of the information. Supervisory Officers may delegate this responsibility to Principals or other Management staff. Supervisory Officers, Principals and Managers are accountable for ensuring staff are informed of the procedures and comply.
- Secondary responsibility for the security of information is vested with 'information systems staff' who manage its processing, transmission, and storage.

Modifications of Hardware and Software

In order for the Board to deliver a high level of service, it is mandatory that the following be followed:

- No staff or students (unless recognized by the Information Technology Department as a Qualified Technician) shall work on the installation, configuration, maintenance or troubleshooting of any board/school computer equipment.
- Only qualified personnel with IT shall administer networks. It is imperative that networks remain a secure environment and therefore only the technicians will retain the passwords for networks, security programs, etc. All passwords will remain within the IT Department. If your computer technician is absent and a problem occurs with your system, please contact the IT Department.
- No staff, unless recognized personnel within the IT Department, shall open computers for any reason. The only exemptions for this are courses, which are designed to teach the inside components of a computer and only equipment that has been donated for this purpose shall be opened.
- Only software approved by the Information Technology Department will be installed on the standalone computers of the school. The Board will endeavour to provide a 'test environment' for software that needs evaluating. Any non-approved software will be removed and reported to the principal at the site.
- If testing is required for the network, a technician must install the software to ensure that it does not negatively affect the network.
- No person outside of the IT Department will install, change or reconfigure any computer or network without the approval of the site technician or the IT Department. No network and/or lab projects will be approved by the IT Department without the full involvement of the school support technicians.
- Software that uses excessive bandwidth and dramatically increases the possibility of virus-infected

files such as, but not limited to, Kazaa (music exchange), ICQ and WinAmp are expressly prohibited.

Compliance and the Disciplinary Process

All employees are expected to comply with the Employees' Acceptable Use of Electronic Access, Information Technology and Data policy. Failure to comply with this policy will result in disciplinary action which may include dismissal.

- In the event that an employee has violated this policy, the employee will be provided with notice of such violation.
- An employee's access to the Board's electronic network may be denied, restricted, or suspended upon any violation of this policy.
- Appropriate legal authorities will be contacted if there is any suspicion of illegal activities.
- The Board will cooperate fully with legal authorities in any investigation relating to illegal activities conducted through the Board's system.
- Employee violation of this policy will be dealt with in accordance with Board policy and procedures.

Amendment

- The Board retains the right to amend and update this policy to conform to new developments in the law.
-

Approved by the Board: June 26, 2001

Amended by the Board: May 25, 2004

Related Policy:

Related Board Committee:

Policy Review Date: 2009