Hamilton-Wentworth Catholic District School Board
Believing, Achieving, Serving

Policy Manual – Administration

A.11 Internet and Technology - Acceptable Use for Employees

POLICY STATEMENT

The Hamilton-Wentworth Catholic District School Board (Board) provides its employees with varied access to the Internet**,** information systems and associated digital communication technologies (i.e., mySite, email, websites, phone system, Wi-Fi, network, devices, etc.) in support of their roles and responsibilities. This policy outlines the acceptable use of the internet, information systems and associated communication technologies through the use of Board-issued devices or when accessing Board digital communication technologies and information systems through personallyowned devices at work or at home. Use of Board digital resources shall be in support of activities consistent with the operation of the Board.

Purpose

The purpose is to ensure that employees use Board-provided internet services and communication technology appropriately and consistent with the mission of the Hamilton-Wentworth Catholic District School Board and the teachings of the Catholic Church. The following principles apply:

- The Board reserves the right to inspect, log, retrieve and archive data stored on Board-issued devices, and data transmitted across its network and communication technologies.
- The Board reserves the right to monitor and audit the use of any Board digital communication technologies, information systems, network/internet traffic, and data at any time;
- No active monitoring, auditing, investigation or disclosure will occur without the direction of Senior Administration;
- Authorized Board Information Communication Technology (ICT) Services personnel may inadvertently view or access data files or messages while performing system maintenance or management functions. When this occurs, they are required to keep the contents confidential, unless there are suspected violations of law or Board policy;
- The Board, as the employer, retains ownership of the entire computer system, including hardware, software, computer system files, documents and electronic communications.
- The Board's communication technologies are not intended for personal use by employees;
- Users of Board-provided internet and communication technologies are responsible for their appropriate use. All illegal and improper uses, including but not limited to bullying, pornography, obscenity, harassment, solicitation, gambling, commercial use, jokes, political lobbying and violating copyright or intellectual property rights are prohibited;

- Emails are not a secure form of communication; thus, emails of a confidential nature should limit the amount of personal identifiable information (PII). PII means recorded information about an identifiable individual including:
- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of an individual;
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual;
- any identifying number, symbol or other particular assigned to the individual;
- the address, telephone number of the individual;
- the personal opinions or views of the individual except where they relate to another individuals; and,
- correspondence that is sent by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contests of the original correspondence.
- Any Board communication that requires the transmission of a confidential document via email shall have the document password protected and encrypted;
- A breach of any terms and conditions of this policy may result in a cancellation of access and further disciplinary action which could include dismissal;
- Employee passwords are to remain confidential. Employees are responsible for all communication originating from their user account;
- Only Board approved applications are to be installed on Board-issued devices;
- Hard-wired connections of non-Board-provided equipment to the network in any school or Board site is not permitted and may be confiscated;
- Users are expected to practice acceptable digital citizenship;
- Use of the Board's communication technologies for activity that relates to, or is in support of illegal activities shall be reported to the authorities; and,
- Any attempts to compromise (hack) Board communication technologies and information systems will be subject to disciplinary actions and may be reported to the authorities.
- Employees are expected to only use Board digital resources and their system access consistent with their employment duties;
- Employees should report any suspected abuse, data breach or security breach of Board information systems or associated digital communication technologies to the Information and Communication Technology (ICT) department;
- The use of any Board digital resources implies the employee has read this policy and agrees to abide by all regulations outlined here.

Responsibility
Director of Education

Regulations
Municipal Freedom of Information and Protection of Privacy Act, RSO 1990

Related Policies
A.12 Personal Mobile Devices (PMDs)
H.M.04 Security Confidentiality and Protection of Personal Information

Related Board Committee
Committee of the Whole

Policy Review Date:
BM Original Policy Approved 01 June 2004
Revisions: 24 June 2008, 21 June 2011, 01 March 2016, 19 November 2019 ,10 March 2023
To be reviewed every five years- 2028