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

Policy Manual – Information and Communication Technology

I.T.02 - Backup and Restore Policy

The mission of Catholic Education in Hamilton-Wentworth, in union with our Bishop, is to enable all learners to realize the fullness of humanity of which Our Lord Jesus Christ is the model.

POLICY STATEMENT

The Information and Communication Technology (ICT) department supports a variety of business and instructional applications used in the process of delivering services to students and staff. A disruption, loss, damage or compromise of ICT systems and data may negatively impact the Hamilton-Wentworth Catholic District School Board's (HWCDSB) reputation and operations, resulting in significant costs to recover. Formal and comprehensive ICT continuity, backup and recovery controls are necessary to mitigate such risks.

Purpose

The objective of this policy is to define formal requirements for ICT continuity, backup and recovery, in order to prevent or mitigate the risk of ICT system disruption or disaster and allow for an efficient recovery of ICT services and data in a timely manner.

This policy is designed to:

- help safeguard HWCDSB technology assets such as data and application software programs in the event of loss or damage, and to reduce the risk of lost time and effort in recreating operational technology tools,

- address data recovery pertaining to one of two scenarios – restoring a state following a disaster (called disaster recovery) and restoring small numbers of files after they have been accidentally deleted or corrupted, and

- establish backup procedures with an emphasis on data recovery.

This policy applies to all ICT systems and/or applications managed by the ICT Department that store, process or transmit information, including network and computer hardware, software and applications.

This policy does not apply to information that is stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices, with the exception of data synchronized with the device and stored on IT servers (such as Outlook emails and contacts). It is to be clearly noted that HWCDSB users should not save sensitive data on their devices to protect against data loss and privacy breach. All sensitive data should be kept on secured HWCDSB network systems.

Guidelines

Servers will be defined as either infrastructure or data containing servers. These will require separate retention schedules as follows:

Infrastructure Servers

- FULL Daily backups are kept for 14 days - 14 copies.
- FULL Monthly backups are kept for 365 days - 12 copies.

Data Containing Servers

- FULL Daily backups are kept for 14 days - 14 copies.
- FULL Monthly backups are kept for 365 days - 12 copies.
- FULL Yearly backups are kept for 1865 days - 5 copies.

Backups will be required to have secured onsite copies and secured offsite copies (cloud storage).

ICT systems that are critical to HWCDSB activities must be clearly identified, as well as the potential risks of disruption that apply to them.

A standard operating procedure (SOP) document managed by ICT will be required outlining the full backup and restore procedures.

Responsibility

Chief Information Officer

Regulations

Ontario Education Act
Freedom of Information and Protection of Privacy Act (FIPPA, 2012)
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, 2007)
Personal Health Information Protection Act (PHIPA, 2004)
Full text versions of these regulations can be found at**:** **http://www.e-laws.gov.on.ca**

Related Policy

A17 Privacy Breach

Related Board Committee

Committee of the Whole

Policy Review Date

BM Original Policy Approved 21 June 2022
Revisions:
To be reviewed every five years