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

Policy Manual – Information & Communication Technology

I.T. 01 – Information Classification 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
Information Classification is a process in which organizations assess the *data* that they hold and the level of protection it should be given (ISO 27001). A data classification system combined with the policies to be defined in this and other policy documents will protect Hamilton-Wentworth Catholic District School Board (HWCDSB) information from unauthorized disclosure, use, misuse, modification, and deletion.

Purpose
This policy helps to address major data-related risks for HWCDSB.

Responsibility:
Every employee who has access to HWCDSB information or information systems is personally responsible for the protection of information that has been entrusted to their care. All employees who encounter sensitive HWCDSB internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily HWCDSB business activities.

The Chief Information Officer is responsible for this policy and its enforcement.

Regulations
ISO/IEC 27001: A.8.2 – Information Classification
Freedom of Information and Protection of Privacy Act (FIPPA, 2012)
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, 2007)

Related Policies
A11 - Internet and Technology - Acceptable Use for Employees
H.M.04 Security Confidentiality and Protection of Personal Information

Related Board Committee
Committee of the Whole

Policy Review Date
BM Original Policy Approved 02 March 2021
Revisions:
To be reviewed every three years

Table of Contents

1.0 Audience for this Policy

The policy is created for intended use by the following audience at HWCDSB. The Board can expand the usage of the policy as applicable.

1. Board Executives at all levels
2. Board of Trustees
3. Human Resources
4. All Managers
5. All ICT personnel
6. All staff

2.0 Policy Scope and Applicability

This information classification policy applies to all information in the possession or under the control of HWCDSB. For example, confidential information entrusted to HWCDSB by the Board of Trustees, employees, students, business partners, suppliers, and other third parties must be protected with this data classification policy. Employees are expected to protect third-party information with the same care that they protect HWCDSB information. No distinctions between the words “data,” “information,” and “knowledge” are made for purposes of this policy.

3.0 Employee Roles and Responsibilities

The term employee is used in policy documents to mean any human resources working for HWCDSB and includes full-time employees, part-time employees, temporary employees, unpaid resources (students, etc.), contractors, and sub-contractors.

3.1 Employee Responsibility

Every employee who has access to HWCDSB information or information systems is personally responsible for the protection of information that has been entrusted to their care. All employees who encounter sensitive HWCDSB internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily HWCDSB business activities. Sensitive information is either **Confidential** or **Highly Confidential** information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

3.2 Approach

A single lapse in information security can have significant long-term consequences. Consistent use of this data classification system is essential if sensitive information is to be adequately protected. Without the consistent use of this data classification system, HWCDSB unduly risks the loss of partner relationships, personal health information of students, families, and staff, etc., loss of public confidence, internal operational disruption, and excessive costs. This policy consistently protects sensitive information:

- no matter what form it takes;
- what technology is used to process it;
- who handles it;
- where the information may be located; and
- in what stage of its life cycle the information may be.

4.0 Access Control

4.1 Need-To-Know Concept

All policy requirements outlined in this document are based on the concept of Need-To-Know. This means that information must be disclosed only to those people who have a legitimate business need for the information.

4.2 System Access Controls

Access to all HWCDSB sensitive computer-resident information must be protected by access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Traditional access control systems employ user IDs and fixed passwords but could also use secure technologies such as dynamic passwords and biometrics. Whatever technology is employed, access must be controlled for each individual based on that individual's need to know. The notion of the need to know includes not only viewing information but other privileges such as modifying information or using the information to complete a transaction.

4.3 Access Granting Decisions

Access to HWCDSB sensitive information must be provided only after the written authorization of the information Owner has been obtained. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates. From an operational perspective, standard templates of system privileges are defined for all job profiles, and Owners approve these privileges in advance. All information access requests must be issued as defined in the current process (e.g. Manager of the employee's position requests the access). Any other special requests for any access privileges other than those granted by the job profiles will be dealt with on a request-by-request basis and must be approved by the information Owner. All new hires, updates to roles and responsibilities, and terminations will be processed through the ICT automated user account identity management system that is linked to the Human Resource information system. The automated user account identity management system will manage the creation of users' active directory account with standard access permissions, permission changes and terminations based on predefined job profiles and the associated start/end dates. Any additional permission requests that are outside of a job profile require approval of the relevant HWCDSB information Owner and the request is to be tracked in the ICT ticket system.

5.0 Classification Labels

5.1 Owner and Production Information

All production information types possessed by or used by a particular organizational unit within HWCDSB must have a designated Owner. Production information is information routinely used to accomplish business objectives. Examples include payroll summaries, student information, and monthly accounting reports. Information Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the HWCDSB management team who act as stewards, and who supervise how certain types of information are used and protected. By default, the owner of an information asset is the creator (person or department) of the information.

Table 1 - Classification Examples for Confidentiality

DESCRIPTION	C3 HIGHLY CONFIDENTIAL	C2 CONFIDENTIAL	C1 INTERNAL USE	C0 PUBLIC
Tombstone data found on enrolment forms, benefit forms, TD1's, Medical data, WSIB	X			
Lawyers information privilege/confidential advice and reports	X			
Core IT Systems access (Active Directory, etc.)	X			
Passwords, Encryption Keys, Digital Certificates	X			
PII (Personally Identifiable Information)	X			
Banking information	X			
Student information (Ontario Student Record)		X		
PHI (Personal Health Information)	X			
Litigious files/documents/items	X			
Disciplinary data		X		
Data contained in recruitment files (drivers abstract info, criminal checks, etc.)		X		
Insurance Policies			X	
Pending Agreements / Ongoing negotiations		X		
Payroll information		X		
Employee Performance Evaluations		X		
Vendor agreement details (pre-selection / pre-vote)		X		
Vendor agreement details (post selection / post vote)			X	
Transaction Details (Bills)			X	
Email (low expectation of privacy)			X	
Voicemail (higher expectation of privacy)		X		
Employee List / Phone Directory			X	
Employee Training Material				X

DESCRIPTION	C3 HIGHLY CONFIDENTIAL	C2 CONFIDENTIAL	C1 INTERNAL USE	C0 PUBLIC
Official HWCDSB Policy Documents				X
Official Marketing Documents / Literature				X
Tax Information				X
Active Contracts				X
Job Postings and Job Descriptions				X
Per contractual obligation	X	X	X	X
Per regulatory / legal obligation	X	X	X	X

5.2 Confidentiality Classification

HIGHLY CONFIDENTIAL (C3)

This classification label applies to the most sensitive business information that is intended for use strictly within HWCDSB. Its unauthorized disclosure could seriously and adversely impact HWCDSB, its students, employees, business partners, and suppliers.

CONFIDENTIAL (C2)

This classification label applies to less-sensitive business information that is intended for use within HWCDSB. Its unauthorized disclosure could adversely impact HWCDSB or its students, employees, business partners, and suppliers.

FOR INTERNAL USE ONLY (C1)

This classification label applies to all other information that does not fit into the previous two classifications. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact HWCDSB or its students, employees, business partners, and suppliers.

PUBLIC (C0)

This classification applies to information that has been approved by HWCDSB management for release to recipients identified by HWCDSB management.

5.3 Other Labels

HWCDSB department or division-specific data classification labels are permissible but must be consistent with and supplemental to the HWCDSB data classification system. These supplementary labels might for example include the use of words like “Private” or “Financial.”

5.4 Owner and Access Decisions

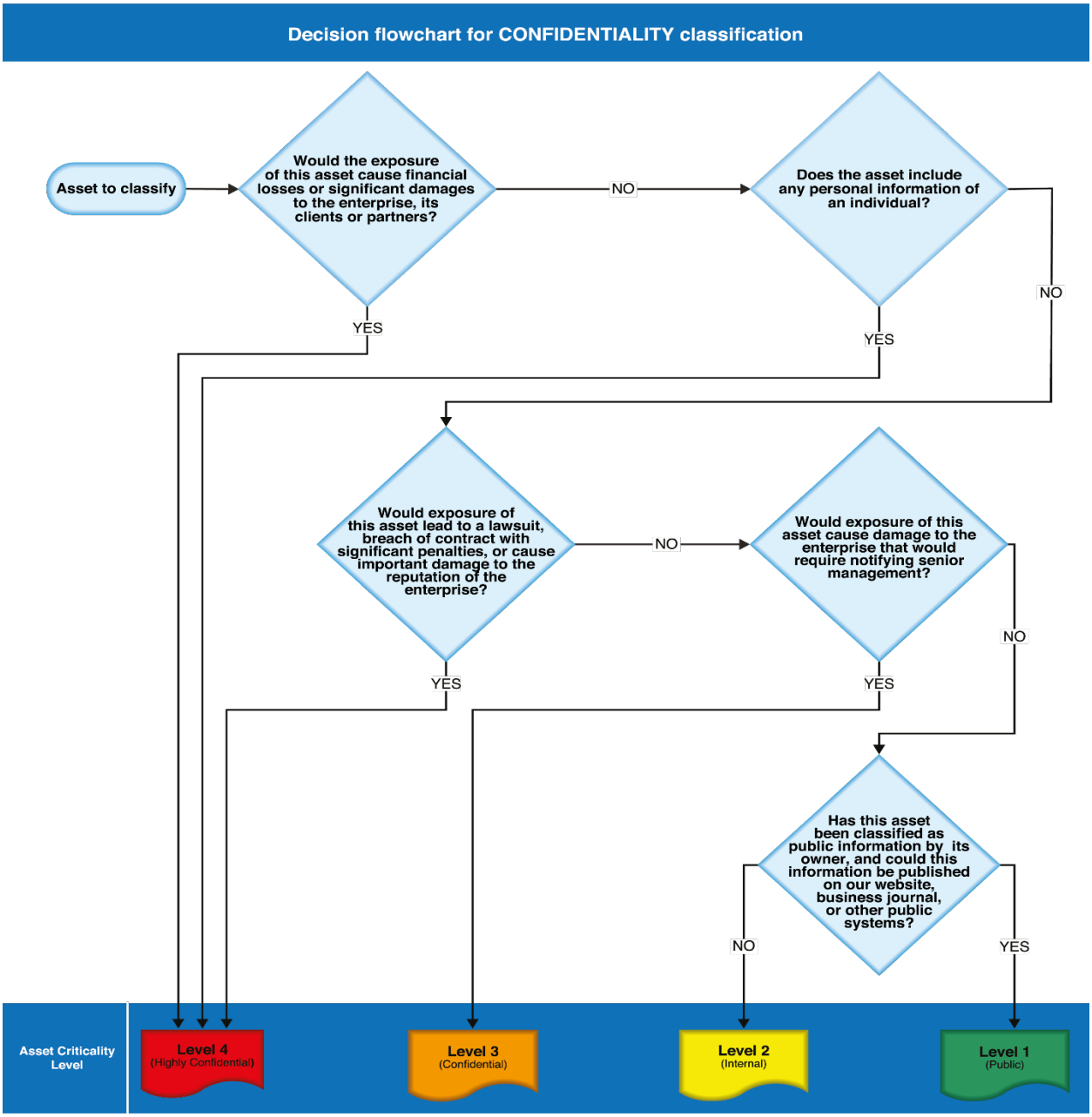
When dealing with Highly Confidential (C3) classified information, owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

6.0 Decision Flowchart

To ensure that two individuals attempting to classify an asset come to the same conclusion, a decision flowchart is proposed that will ask clear and simple questions that orient the user to the appropriate classification level.

Additional flow charts should be developed and enhanced as time progresses to include enterprise-specific examples within the diagrams to facilitate the comprehension of what falls under which level of criticality. As this policy is at its infancy, the following flowchart will serve as a recommended template:

Figure 1: Decision Flowchart for CONFIDENTIALITY classification



7.0 Third-Party Interactions

7.1 Third Parties and The Need-To-Know

Unless it has been specifically designated as Public, all HWCDSB internal information must be protected from disclosure to third parties. Third parties may be given access to HWCDSB internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorized by the relevant HWCDSB information Owner. Contractors, consultants, temporaries, volunteers, and every other type of individual or entity that is not an HWCDSB employee, is by definition a third party for purposes of this policy.

7.2 Disclosures from Third Parties and Non-Disclosure Agreements

The receipt of a signed HWCDSB non-disclosure agreement must precede disclosures of sensitive information to Third Parties such as consultants, contractors, temporaries, or any other external resources. Employees must not sign non-disclosure agreements provided by third parties without the authorization of HWCDSB legal counsel designated to handle intellectual property matters. These forms may contain terms and conditions that unduly restrict the future business directions of HWCDSB.

7.3 Third-Party Requests for HWCDSB Information

Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about HWCDSB and its business must be referred to Public Relations. Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about HWCDSB products and services, nor does it pertain to customer support calls.

7.4 Owner Notification

If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and the Chief Information Officer must be notified immediately.

8.0 Physical Security

8.1 Offline Access

Access to every office, computer room, and work area containing sensitive information must be physically restricted. Only authorized individuals or accompanied visitors may have access to HWCDSB premises.

8.2 Locked When Not in Use

When not in use, sensitive information must be protected from unauthorized disclosure. When left in an unattended room not assigned for the storage of such information, such information must be locked in appropriate containers. If a Custodian of such information believes he or she will be away for less than 30 minutes, the information may be left on a desk or in some other readily observed spot only if all doors and windows to the unattended room are closed and locked.

8.3 Unauthorized Screen Viewing

The screens on computers used to handle sensitive information must be positioned such that unauthorized persons cannot readily look over the shoulder of the person using the workstation. Screens should be positioned such that sensitive information cannot be seen through windows.

9.0 Special Consideration for Highly Confidential Information

9.1 Background Checks

All employees who will have access to Highly Confidential information must have passed a standardized background check performed by the Human Resources department. Access to Highly Confidential information must not be provided before this background check is completed.

9.2 Storage on Personal Computers

If Highly Confidential information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must support storage (disk, etc.) encryption. When these users are not currently accessing or otherwise actively using the Highly Confidential information on such a machine, they must not leave the machine without logging off, invoking a locked screen saver, or otherwise restricting access to the Highly Confidential information.

9.3 Storage

Highly Confidential information must make use of encrypted storage unless a risk assessment has concluded that the target architecture does not warrant encryption.

9.4 Transmission Over Networks

If HWCDSB Highly Confidential data is to be transmitted over any communication network, it must be sent only in encrypted form. Such networks include internal electronic mail systems, the Internet, and unified communication and collaboration software (e.g. Microsoft Teams). All such transmissions must use an encrypted virtual private network (VPN) or similar software as approved by the Information Communications Technology Group.

9.5 Fax Transmission

Highly Confidential information must not be sent to an unattended fax machine unless the destination machine is in a locked room for which only people authorized to receive the information possess the keys. Transmission to a fax server that uses passwords to control access to receive faxes is a permissible exception to this policy assuming that the information owner has approved the transmission to the target destination.

9.6 Conference Calls (telephone bridges)

Employees must avoid disclosing Highly Confidential information on conference calls. Conference calling systems can be monitored, can record sessions, and are sometimes outside of HWCDSB control (not an HWCDSB system), this can lead to a significant security exposure. When Highly Confidential information must be discussed, employees should use only HWCDSB conferencing systems and should ensure that each participant on the line has been validated.

10.0 Exceptions

The HWCDSB ICT Security Lead acknowledges that under rare circumstances, certain employees will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the Chief Information Officer and the Associate Director of Corporate Services.

11.0 Violations

HWCDSB employees who willingly and deliberately violate this policy will be subject to progressive disciplinary action up to and including termination.