DURHAM CATHOLIC
DISTRICT SCHOOL BOARD
Learning and Living in Faith

POLICY – 400

Cyber Security

Area: Operations
Source: Chief Information Officer – Freedom of Information and Privacy

Approved:
Revised:

1. Introduction

The Board is committed to protecting its information systems and data from unauthorized access, use, disclosure, modification or destruction, and to complying with all applicable laws and regulations regarding cyber security. The Board recognizes that cyber security is a shared responsibility that requires the cooperation and collaboration of all users of the Board's network and devices. The Board also acknowledges that cyber threats are constantly evolving and may pose significant risks to the Board's operations, reputation and legal obligations.

2. Definitions

Nil

3. Purpose

The purpose of this policy is to establish the Board's guidelines for computer security and the protection of its network, its content or knowledge base, and to minimize the risk of internal and external cyber threats.

4. Application / Scope

This policy and its attendant administrative procedures apply to all users of the Boards' network and devices, including Trustees, staff, students, contractors, vendors, volunteers and visitors. It also applies to all information systems and data owned, operated, leased or controlled by the Board, regardless of their location or format.

This policy does not supersede or replace any other policies or procedures that the Board may have in place. In case of any conflict or inconsistency, the more restrictive policy or procedure shall prevail.

5. Principles

5.1 The Board is committed to:

5.1.1 identifying and managing cyber security risks, establishing the roles and responsibilities of the users and stakeholders, and providing the leadership and oversight of the cyber security program. (Govern)

5.1.2 securing configurations, networks, systems and data, applying the principle of least privilege, implementing fail-safe defaults, and following the economy of mechanism (i.e, security mechanisms should be as simple as possible, and entities should only be granted the minimum system resources that they need to perform their function). (Protect)

5.1.3 monitoring the activities, events and anomalies on the network and systems and reporting any incidents or breaches. (Detect)

5.1.4 having a clear and effective incident response plan, following the principle of complete mediation, and implementing the corrective and preventive measures. (Respond and Recover)

6. Requirements

6.1 The Director of Education, or designate, shall issue administrative procedures to support this policy and amend them thereafter as the need may arise.

6.2 All users must practice due diligence in controlling access to their systems by protecting their user accounts with passwords that are not easily guessed or deduced. User passwords must not be shared with anyone, and/or not written down.

6.3 All staff and Trustees must have multi-factor authentication enabled on all applications where Board data is accessed.

6.4 The Board shall:

6.4.1 operate its information and operational technologies in a secure, vigilant, and resilient manner that minimizes cyber risks to its information assets and facilities.

6.4.2 establish and maintain a management system that reduces cyber risk, protects critical information and operational technology assets in accordance with cyber security standards, while, at a minimum, maintaining compliance with legal and regulatory requirements.

6.4.3 ensure employees, contractors and suppliers comply with all applicable requirements in the management system.

6.4.4 cultivate a culture of awareness that promotes secure practices in the use of all technologies and information assets.

6.4.5 take appropriate steps to monitor its information and operational technologies on an ongoing basis to detect, and respond to, threats that impact the confidentiality, integrity, and availability of its assets.

6.4.6 ensure strategies are in place to prepare for, respond to, and recover from cyber security incidents that impact its reputation and public and employee safety.

6.5 Remote employees are also obligated to comply with this policy in the use of the Board's systems, equipment, and confidential data.

7. Sources

Nil

8. Related Policies and Administrative Procedures

8.1 Acceptable Use of Information and Communications Technology Policy (PO431)
8.2 Acceptable Use of Information and Communications Technology Administrative Procedure (AP431-1)
8.3 Freedom of Information and Protection of Privacy Policy (PO201)
8.4 Privacy Breach Protocol Administrative Procedure (AP201-2)
8.5 Data Access and Management Policy (PO427)
8.6 Data Access and Management Administrative Procedure (AP427-1)