#17 Cyber Security
BOARD POLICY

Board Approval:	February 28, 2024
Effective Date:	March 1, 2024
Amendment Date:	N/A
Review Date:	March 1, 2027

PURPOSE

All Stakeholders of HLG are responsible for protecting and maintaining the integrity and stability of HLG's Information Technology (IT) and Internet of Things (IoT).

DEFINITIONS

Headwater Learning Group, HLG – the term for three independent charitable organizations: Calgary Academy Society, Headwater Learning Foundation, and Headwater Learning Solutions Foundation.

Internet of Things, IoT – refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

Information Technology, IT – refers to HLG's networks, hardware, software, and data storage and the management systems that apply to them.

Stakeholders – students, employees, representatives, contractors, parents, alumni, board members, community members, or individuals who share a common interest in HLG.

Representatives – directors, employees, service providers and contractors of HLG.

Employee – an individual who is working under an employment relationship with HLG.

Contractor – an individual or company hired under a contract to provide specific services for HLG.

Student – an individual currently enrolled at Calgary Academy.

GUIDELINES

1. HLG acknowledges the importance of safeguarding confidentiality, integrity, and availability of its IT and IoT systems. By ensuring their security, we maintain the uninterrupted operation of critical infrastructure, bolster financial and business transactions, safeguard data, and maintain compliance with legal and regulatory requirements.
2. HLG endeavours to protect its IT and IoT against unauthorized access and disclosure the confidentiality of information through industry-leading responses and prevention.
3. All stakeholders share the responsibility of ensuring the safety and integrity of HLG's IT and IoT systems by proactively identifying risk and reporting incidents of concern as soon as possible.
4. All Stakeholders that have access to HLG's IT and IoT will be required to comply with learning and development training, as per outlined frequency in a relevant procedure, related to security risks.
5. HLG's IT department will identify information security responsibilities, regulatory and legal requirements, and methods to integrate them into HLG policies, procedures, and processes where appropriate.

REFERENCES

Personal Information Protection Act, SA 2003 c.P-6.5 (PIPA)

Personal Information Protection Act Regulation 366/2003 Dec 12, 2018

CROSS-REFERENCES

F.01 – Responsible Use of Technology

F.06 – Emergency Preparedness

F.08 – Incident Reporting and Investigation

P.11 – Digital Citizenship

P.05 – Code of Conduct