

**Appendix A: Administrative Procedure 512, Electronic Monitoring**

<b>Tool</b>	<b>What is monitored?</b>	<b>How</b>	<b>Purpose</b>
Web filtering	All internet traffic	Firewalls	Protect from harmful and inappropriate content
E-Mail filtering	All e-mail traffic	Safety and Security	Prevent the transmission of inappropriate/confidential data over insecure e-mail
Network Monitoring	All network traffic	Packet analysis	Protect the integrity and availability of the network
Account Authentication	Staff login to services	Authentication Server	Protect against unauthorized access
Device Management (iPad/iPhone)	Installed on all Board iPads/iPhones	Mobile Device Management	Protect against loss/ theft, and enforce security settings
Device Management (Chromebook)	Installed on all Board Chromebooks	Management Console	Protect against loss/ theft, and enforce security settings
Device Management (laptop)	Installed on one-to-one/ administrative laptops	Endpoint Security Tool	Protect against loss/ theft, and enforce security settings
Phone logs	Some facilities	Private Branch Exchange (PBX) phone system	Call quality (e.g. bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage monitoring
Video surveillance	Some facilities	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioural/ incident monitoring and review as described in AP 1208 - Video Surveillance Systems at Board Facilities.
Access Cards	All facilities	Through Door Reader	Control and monitor access to buildings.
Electronic sign-in	Some facilities	Electronic data collection	Maintaining a Visitor's Book per the Education Act and where necessary for health related purposes.