Auditor General of Ontario – School Board IT Systems and Technology in the Classroom Follow Up Audit Update

To: Audit Committee

Date: 22 March, 2021

Report No.: 03-21-4050

Strategic Directions

- Allocate Human and Financial Resources Strategically to Support Student Needs

Recommendation

It is recommended that the Auditor General of Ontario – School Board IT Systems and Technology in the Classroom Follow Up Audit Update be received.

Context

In 2018 the Auditor General of Ontario (OAGO) conducted an audit on School Board IT Systems and Technology in the Classroom. As part of the original audit the Ministry of Education (EDU) and four school boards, TDSB, Waterloo Catholic School Board, Algoma District School Board and Peel District School Board were selected to audit. A follow up audit was conducted in 2020 with the report being issued in December 2020. The Board has recently been informed that the Auditor General will be conducting School Board IT Systems and Technology in the Classroom follow up audits on an annual basis going forward; this update relates to the follow up audit report published in December 2020. Management is in the process of providing the 2021 update due March 31st, 2021.

The original report contained 14 recommendations consisting of 26 action items. Of the 14 recommendations, nine were addressed to the school boards resulting in 17 action items. The Auditor General conducted their follow up from May to July 2020, releasing their report in December 2020. The follow up concluded that TDSB had fully completed seven of the 17 action items with six additional action items to be completed by the end of the current school year. One action item will not be completed as it is cost prohibitive (the Board is willing to partner with EDU on a provincial solution), however compensating controls have been introduced and three action items relating to disaster recovery and business continuity have made little to no progress. It should be noted that backup procedures are in place; cold sites have been identified and a fulsome assessment of how to move to a full BCP and DRP is in the process of being

developed. However, given the current budgetary constraints and lack of dedicated funding, implementation is taking longer than anticipated.

School Board Recommendations and Current Status (as of February 2020):

Recommendation 2: In order to achieve more equitable access to classroom IT resources, Boards are recommended to perform (a) an assessment of student needs and (b) implement policy outlining device allocation, type of technology, refresh cycle etc. Due March 2021.

Current Status: **In Process** – Assessment to evaluate student needs re: classroom technology has been completed. It was determined that a 1 to 1 student to device strategy be implemented along with teacher PD as well as digital resources. The proposal is a work in progress to establish a sustainable funding model.

Recommendation 3**:** Investigate the benefits of donations of used equipment. Due March 2021.

Current Status: **Fully Implemented** – The board has a bring your own device (BYOD) program in place where students and staff can use their personal devices to engage in learning and collaboration in their classrooms by connecting to the Boards Wi-Fi network (login credentials required).

Recommendation 4: Periodic review of users with access to the Ontario Education Number applications so EDU can be notified of those no longer requiring access.

Current Status: **Fully Implemented** – Users lists are reviewed semi-annually with notification sent to EDU to revoke access for users who no longer require access.

Recommendation 5: Safeguard students' personal information by (a) delivering on-going privacy training to staff with access to personal data and (b) perform risk assessments and necessary actions with use of non-approved websites or software.

Current Status: (a) **In Process (2020)** – All staff are required to complete and obtain a passing grade in the Boards online Municipal Freedom of Information and Protection of Privacy Act training. **2021 update**: Privacy Training is ongoing and made available to all staff through the Learning Management Platform which contains 39 privacy related courses. (b) **Fully Implemented** – The board has been performing cyber-risk assessment on IT systems and initiatives including privacy assessments and has filtered or blocked websites that are deemed high risk.

Recommendation 6: To mitigate the risk of cyberattacks, (a) develop Board and school level roles and responsibilities for cybersecurity and (b) provide formal information security training to teachers and staff.

Current Status: (a) **Fully Implemented** – Roles and responsibilities for cybersecurity, code of online conduct, password management, network security and acceptable use of IT resources are in place. (b) **In Process**: cybersecurity awareness campaigns and phishing exercises provided to teachers and staff, the board was

planning to launch a Cyber-Monday program where cybersecurity and online risks would be taught to
students on the first Monday of every month during the school year, starting January 2021. **2021 update**: The 'Cyber Monday' initiative is on hold due to the continued strain on internal resources, however other awareness initiatives are on-going including cybersecurity training made available to all staff through the Learning Management Platform which contains six cybersecurity related courses. An External Threat Intelligence Software as a Service (SaaS) solution is currently being used to provide early warnings and imminent threats to TDSB and reduce the security risk posture of TDSB.

Recommendation 8: Improve existing cyberbullying programs by (a) monitoring school provided equipment to mitigate cyberbullying incidents and (b) formally track, report and review cyberbullying incidents at schools.

Current Status: (a) **Not Implemented** – Management engaged vendors to understand the implementation and on-going costs of monitoring communication on school provided equipment and determined it is cost prohibitive unless dedicated funding can be identified. TDSB remains willing to collaborate with EDU on a provincial solution. **2021 update**: Although monitoring actual communications is cost prohibitive, TDSB has implemented firewalls and internet content filters to block various high-risk unapproved content including:

- Social Networking User communities and sites where users interact with each other, post messages, pictures, or otherwise communicate with groups of people.
- Internet Communications and Telephony Sites that support or provide services for video chatting, instant messaging, or telephony capabilities.
- Peer-to-Peer Sites that provide access to or clients for peer-to-peer sharing of torrents, download programs, media files, or other software applications. This is primarily for those sites that provide bit torrent download capabilities.

These controls are in place for all devices accessing TDSB networks, this includes BYOD when logged into the TDSB Wi-Fi network.

Item (b) **Fully Implemented** – e-solution application implemented to track and report cyberbullying incidents.

Recommendation 9: Maintain security of and reduce loss due to lost / stolen IT assets by (a) implementing an IT Asset management system with clear roles and responsibilities as well as life-cycle management; and (b) implement format IT asset tracking and reporting procedures.

Current Status: (a): **Fully implemented** – ITSM ServiceNow tool in place which tracks IT equipment information, associated to the serial number of the devices that are shipped in the ITSM module, along with service warranty information. (b): **In Process** – Reporting templates are being finalized based on the information compiled in the tool. **2021 Update**: The ITSM application is used in association with SCCM and MDM apps to determine last login times to better track assets.

Recommendation 10: Develop and test Disaster Recovery Plan.

Current Status: **Little to no progress** – The board was in the process of developing a business continuity and disaster recovery plan at the board and school levels including the necessary assignment of roles and responsibilities, as well as training and testing exercises. However, the board had encountered financial challenges with budget cuts in the 2019/20 school year as well as the added budgetary pressures in 2020/21. **2021 Update**: The Board has engaged a 3rd party consultant company to assist with a guided implementation to create a DRP followed by a BCP. Work has begun and will be on-going.

Recommendation 11: (a) Develop and implement business continuity plans and (b) establish backup schedules, retention policies as well as disposal and security policies and practices.

Current Status: **Little to no progress** – Plans to perform business impact analyses as well as assessing risks and determining prevention and mitigation measures in place. **2021 Update**: BCP will be developed after completion of the DRP as noted in #10 above. Record retention policies, and disposal and security policies and practices in place include: Records and Information Management Policy (PO97) and Records and Information Management Procedure (PR677). For System Backup, IT Services performs regular backups of server configuration, application data, databases, staff/department storage and the administrative email mailboxes on a daily basis. Incremental backups are performed daily and retained for 4 weeks; full backups are performed at the end of the week and retained for a 1-year period. Copies of full backups are kept offsite for 3 weeks.

Recommendation 12: Ensure teachers and staff (a) receive necessary training to use technology purchased and (b) perform a cost-benefit analysis of equipment and software prior to making purchases.

Current Status: (a) **In Process**: Online and in-person technology-related training provided to teachers and staff through the training website during the 2019/20 school year. The training website is available to all teachers and staff and provides training courses for the use of technology in classrooms and at the board. The training website also tracks formal learning sessions for monitoring training completion status with the course contents regularly reviewed for appropriateness. **2021 Update**: To assist in building capacity, PD sessions were held for Digital Lead Learners and Digital Lead Administrators (DLL and DLA) on Digital Citizenship and Global Competencies in February and March of 2021.
Targeted teacher training will be held in co-ordination with the 1 to 1 Computing Strategy noted in #2 above. (b): **Fully Implemented** – cost / benefit analysis included in for equipment and software purchases.

Action Plan and Associated Timeline

Of the remaining nine action plans, all of which are being addressed, six action plans are anticipated to be completed prior to the beginning of the 2021 school year. For the

remaining three actions, work has commenced to address the findings within the Boards budgetary constraints.

Resource Implications

No additional resource implications are anticipated to address the six action plans brought forth by the OAGO, however until dedicated funding or provincial solutions are provided, completion of three action items will remain outstanding.

Communications Considerations

Included in public Audit Committee minutes.

Board Policy and Procedure Reference(s)

N/A – O.Reg 361/10 and Auditor General Act of Ontario are applicable.

Appendices

- Appendix A: OAGO School Board IT Systems and Technology in the Classroom Follow Up Audit

From

Peter Singh, Executive Officer, Information Systems and Information Management, at Peter.Singh@tdsb.on.ca or 416-396-5700

Sandy Lew, Senior Manager, Application Management & Business Operations at Sandy.Lew@tdsb.on.a or 416-396-6248