Committee of the Whole (Public) **18 February 2020**
Report 20-020

Policy P.074.IT Computer Network Security
Key Contact: Shawn Lehman, Superintendent of Instruction, ext. 8391

PURPOSE:

1. To seek approval of the proposed revisions to Policy P.074.IT Computer Network Security (attached as Appendix A).

CONTEXT:

2. The Board last approved Policy P.074.IT Computer Network Security in January 1999. The digital security landscape has evolved considerably during the last 20 years. While technology has to continually evolve to mitigate the technological threats, there is a greater need for awareness for staff and students to be cognizant of threats via social engineering, phishing attacks, email spoofing, etc. The revisions to the computer network security policy will help to minimize threats to the District's infrastructure and data that we hold. The Security Steering Committee recommended that the policy, which was last updated in 1999, be revised. A consultation plan (attached Appendix B) was presented to Committee of the Whole on 1 October 2019. This report is presented for approval of the revise policy which has been updated to include the input received through the consultation.

KEY CONSIDERATIONS:

3. **Policy Direction**
Trustees provided feedback at the 1 October Committee of the Whole meeting regarding the policy and the consultation process. The Committee feedback suggested a need to ensure the policy expressed the Board's commitment to security of information technology and established broad level parameters for the implementation of security standards and practices which could be document in the procedure. The Committee also advised that in addition to the public consultation, it was essential that staff seek the advice of an independent

professional third party with expertise in this area. This direction and the feedback from the consultation has informed the revisions leading to a revised policy (Appendix C) reflects that feedback. Many of the struck items will be incorporated into the procedure. The Operational Steering Committee is currently working on revising the accompanying procedure(s).

Audit Committee spoke to the need for cadence in the policy as cybersecurity and the technology landscape is constantly evolving. It was recommended that the policy be reviewed at least every 3-5 years to ensure it meets the District's needs. The Committee also recommended that benchmarks such as NIST Cybersecurity Framework 1.1 and ISO/IEC 27001:2013 be consulted and referenced. These frameworks were consulted and considered during the consultation period. In addition to these frameworks, the Government of Canada website, Get Cyber Safe.org was consulted.

As part of the review process, staff worked with our external third party service provider who recently undertook a review of IT operations and who is providing support to the further development of our security infrastructure. The consultant has encouraged the streamlining of the policy and the development of more detailed operational practices and standards which can be responsive to the changing issues in the security landscape.

The revised policy must be considered as part of a set of policy directives, including the Appropriate Use Policy, the Privacy Policy and the Electronic Communications Policy. Work will continue to align and integrate these documents and the supporting procedures.

4. **Security Governance**

The Security Steering Committee was formed as per the recommendation of the 10 Essential Security Assessment. The first recommendation of the Security Steering Committee was to update the Computer Network Security policy and review the accompanying procedures.

5. **Awareness and Training**

One of the key changes to this policy is the commitment of the District to provide training to all staff. Security awareness training can occur in a variety of forms including online modules, simulated phishing attacks with responses to educate the user, and face to face workshops. Baseline data will be gathered and used to assist with planning future training opportunities and monitoring the impact. The three year technology plan "Transforming How we Learn and Work" highlights privacy and security as a priority. Business and Learning Technologies (B&LT)

will focus its resources in the form of a dedicated Security team to prioritize the protection of the District's assets.

6. **Third Party Data Sharing**
With the increase in availability of third party applications for educational use, teachers are being asked to interpret privacy agreements and terms and conditions before sharing student data. This has been a challenge for educators and it is clear they are in need of guidance and support in this area. The District is moving forward with the creation of a software catalogue committee that will curate, oversee and recommend applications in schools from a pedagogical, technological and privacy and security perspective. The District will be collaborating with other districts through the Ontario Association of School Business Officials (OASBO) and through the Educational Computing Network of Ontario to provide consistency to the process.

7. **Privacy and Security**
Privacy and security have a reciprocal relationship. While information management security and privacy are an important part of a secure infrastructure, the District has an established privacy policy that will complement the proposed security policy. Security refers to how information is protected while privacy refers to the permissions assigned to information being shared.

8. **Title of Policy**
Feedback during the consultation process indicated that the title "Computer Network Security" was too limiting. To reflect the emphasis for security across all aspects of information technology the policy is being renamed "Information Technology Security".

RESOURCE IMPLICATIONS:

9. The resources required to carry out this work will be part of the B&LT department budget.

COMMUNICATION/CONSULTATION ISSUES:

10. After the consultation plan was approved by Committee of the Whole on 1 October 2020, information related to the Computer Network Security consultation was sent to all school councils through the school council newsletter and to all parents through Keeping You Connected, as well as posted to the District's website. Interested parents and members of the community were invited to share feedback either electronically or at a planned policy discussion meeting held on 12 November 2019.

In addition, consultation included targeted outreach to the federations, the Audit Committee, principals, vice-principals and managers, students, and staff in B&LT.

B&LT reviewed the feedback provided through the consultation and engaged a third party consultant, IBM, to review the policy revisions, feedback from trustees and to conduct a gap analysis between the policy and best practices.

Students in grades 7-12 at three different schools were consulted via focus groups. Overall feedback from students focused on the importance of regular security training for staff and students.

While a community focus group was not well attended, there was feedback provided from both community and staff through the online survey. This feedback was varied but emphasized the need for a robust secure policy to ensure the protection of District data.

Once approved, the revised policy will be shared with staff via a system memo. It will also be posted on the district website and will be highlighted in the staff portal.

STRATEGIC LINKS:

11. This policy revision is aligned with a Culture of Caring through championing and nurturing a safe, caring and respectful workplace.

RECOMMENDATION:

THAT the revisions to Policy P.074.IT - Information Technology Security (attached as Appendix A to report 20-020) be approved.

_____ _____

Shawn Lehman
Superintendent of Instruction

Camille Williams-Taylor
Director of Education
Secretary to the Board

Appendix A - Current online Policy P.074.IT
Appendix B - Pre-Consultation Version
Appendix C - Post-Consultation