

### Public Notice – Board of Education Online Public Meeting

A public meeting of the Education-Policy Committee for School District 62 (Sooke) **will be held on Nov. 8, 2022 at 6:00 pm.**


**Please note that all Public Board and Committee meetings are now held in person at the District School Board Office, located at 3143 Jacklin Road, Victoria.**

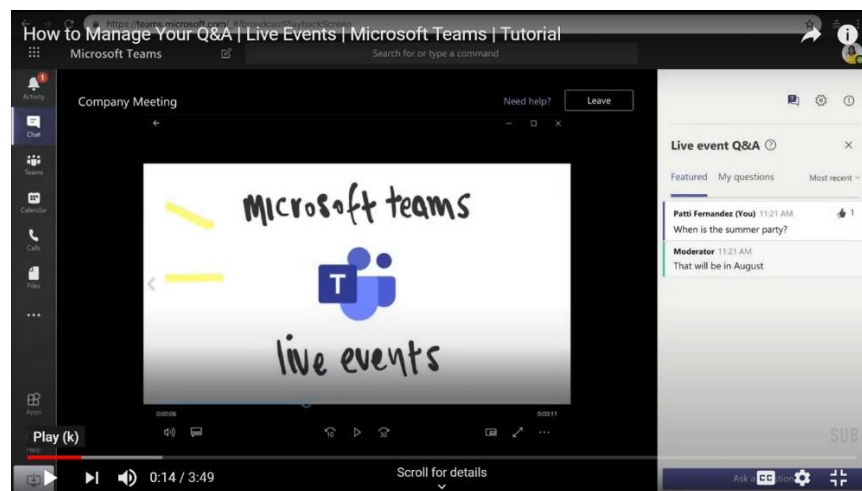
Furthermore, the meeting will be livestreamed via MS teams, to encourage more public participation.

To participate in the meeting please click on this link: <https://jump.sd62.bc.ca/Education-PolicyCommittee-Nov-8-2022>

To guide you, the following is information on how to join a live event in MS Teams.

<https://support.office.com/en-us/article/attend-a-live-event-in-teams-a1c7b989-ebb1-4479-b750-c86c9bc98d84>

- Anyone who has the link can attend the online meeting without logging in to MS Teams.
- Members of the public have the opportunity to ask questions related to agenda items discussed at the meeting:
  - Select the **Q&A**  function on the right side of the screen.
  - When asking a question using the Q&A function, please identify yourself. **Anonymous questions will not be responded to.**
    - A reminder for Stakeholder groups to use the **Q&A** function.
  - Members of the media can direct their questions to the Communications Manager at School District 62 for response following the meeting.



If you have questions regarding the meeting and how to access it that aren't answered in the link above please email [info@sd62.bc.ca](mailto:info@sd62.bc.ca).



**EDUCATION-POLICY COMMITTEE**  
**School Board Office**  
**Via MS Teams**  
**November 8, 2022 – 6:00 p.m.**

---

**A G E N D A**

1. **CALL TO ORDER AND ACKNOWLEDGMENT OF FIRST NATIONS TERRITORIES**  
*We are honoured to be meeting on the traditional territories of the Coast Salish: T'Sou-ke Nation and Sc'ianew Nation and Nuu-chah-nulth: Pacheedaht Nation. We also recognize some of our schools reside on the traditional territory of the Esquimalt Nation and Songhees Nation.*
2. **Opening Remarks from Acting Chair, Ravi Parmar**
3. **COMMITTEE REPORT** of Oct. 4, 2022 Education Standing Committee meeting (attached) **Pg. 3**
4. **BAA COURSE PROPOSALS**  
 There are no BAA course proposals for this meeting.
5. **REVIEW OF POLICIES/REGULATIONS** (attached)
  - a. Draft New Policy and Regulations F-325 "Cyber Risk and Security" – review of revisions – Farzaan Nusserwanji **Pg. 6**
6. **NEW BUSINESS** (attached)
  - a. Quarter 1 Report on Strategic Plan – Scott Stinson **Pg. 27**
  - b. Update – Student & Family Affordability Fund – Dave Strange **Pg. 56**
7. **FOR INFORMATION**
  - a.
8. **FOR FUTURE MEETINGS**
9. **ADJOURNMENT AND NEXT MEETING DATE:** Dec. 6, 2022



**COMMITTEE REPORT OF THE  
EDUCATION-POLICY COMMITTEE via MS Teams  
School Board Office  
October 4, 2022 – 6:00 p.m.**

---

Present: Margot Swinburnson, Trustee (Acting Committee Chair)  
Diana Seaton, Trustee  
Bob Beckett, Trustee  
Ed Berlando, STA  
Lou Leslie, CUPE  
Sandra Arnold, SPEAC  
Shannon Miller, SPVPA  
Scott Stinson, Superintendent/CEO  
Monica Braniff, Associate Superintendent  
Dave Strange, Associate Superintendent  
Paul Block, Associate Superintendent

Guests: Christine Merner, Denise Wehner, Stephanie Cave, Nicole Wallace, Sarah Bass

Regrets: Allison Watson

1. **CALL TO ORDER AND ACKNOWLEDGMENT OF FIRST NATIONS TERRITORIES**

*We are honoured to be meeting on the traditional territories of the Coast Salish: T'Sou-ke Nation and Sc'ianew Nation and Nuu-chah-nulth: Pacheedaht Nation. We also recognize some of our schools reside on the traditional territory of the Esquimalt Nation and Songhees Nation.*

2. **Opening Remarks from Acting Chair, Margot Swinburnson**

3. **COMMITTEE REPORT** of Sept. 6, 2022 Education-Policy Committee meeting

The committee report for the Sept. 6, 2022 Education-Policy Committee meeting was reviewed by the committee. No errors or omissions were noted.

4. **BAA COURSE PROPOSALS**

There are no BAA course proposals for this meeting.

5. **REVIEW OF POLICIES/REGULATIONS** (attached)

- a. Draft New Policy and Regulations C-434 "Universal Precautions" – Dave Strange and Christine Merner Associate Superintendent Dave Strange and Christine Merner, Manager – OH&S, explained the rationale for rescinding Policy and Regulations C-433 "HIV Virus (A.I.D.S.)". This followed with an explanation surrounding the introduction of Draft new Policy and Regulations C-434 "Universal Precautions". A discussion about the meaning of the term "Universal Precautions" and about training

opportunities for staff occurred. Some minor edits were suggested and will be incorporated into the final version for Board approval.

**Recommendation:**

That the Board of Education for School District #62 (Sooke) RESCIND Policy and Regulations C-433 “HIV Virus (A.I.D.S.)” and remove them from the District’s Policy manual.

That the Board of Education for School District #62 (Sooke) give Notice of Motion to draft new Policy and Regulations C-434 “Universal Precautions”.

- b. New Regulations F-204 “Naming of Schools” – Paul Block  
Associate Superintendent Paul Block discussed the passing of the revised Policy in June 2022 which lead to the development and introduction of new Regulations to support staff and community by providing clarity of process with an emphasis on consultation with all partners, students, staff and community and or First Nations. The new Regulations were brought forward for information.
6. **NEW BUSINESS** (attached)
- a. Presentation – “Library Learning Commons Philosophy” – Denise Wehner and Dave Strange  
Dave Strange and Denise Wehner, District Principal – Curriculum Transformation, introduced a dynamic group of educators to lead the committee in a conversation about Learning Commons in our district.
- Stephanie Cave, Sarah Bass and Nicole Wallace (teachers) led the committee through a presentation that spoke to a new District philosophy for Learning Commons (previously known as libraries) that will assist staff in maximizing the resources and opportunities available to students and staff in our schools.
- Discussion regarding the philosophy, resourcing and the transition process from a traditional academic library setting to a Learning Commons occurred.
- Superintendent Scott Stinson encouraged the educators, with Denise and Dave’s support, to consider returning to the committee with a refined Learning Commons philosophy with the intent to request a motion from the Board of Education acknowledging the work and endorse the aspects of the learning commons district-wide.
- c. Update – Planned Spending – Student & Family Affordability Fund – Dave Strange  
Dave Strange provided a brief summary to the committee of the Student & Family Affordability Fund guidelines and the subsequent development of a draft SD62 implementation plan for feedback from committee.
7. **FOR INFORMATION**
- a. Research Project Approval – Oyebisi Fawole – “A Case Study of Teachers’ Beliefs in Supporting Grade Four English Language Learners’ Reading Proficiency”
- b. Research Project Approval – Heather Finlay – “A Multi-Perspective Study of Effective Learning for Students with Extensive Support Needs”
- c. Research Project Approval – Rachelle Hole – “The Transitioning Youth with Disabilities and Employment Project”
8. **FOR FUTURE MEETINGS**

9. **ADJOURNMENT AND NEXT MEETING DATE:** Nov. 8, 2022

DRAFT



**Information Note**  
**Education-Policy Committee Meeting**  
**Nov. 8, 2022**  
**Agenda Item 5a: New Board Policy and Regulations**  
**F-325 "Cyber Risk and Security"**

---

### **Purpose**

- To provide an update to the Education Policy committee on the revisions and due diligence conducted on the Cyber Risk and Security Policy based on questions and feedback from the September Education Policy Committee meeting.
- To confirm that the revisions meet the feedback from partners and trustees and represent the risk tolerance of the Board.

### **Context and Background**

- Audit Committee via internal auditors identified that the overall audit rating for controls with respect to Information Technology (IT) Security is **"Inadequate"**.
- The audit noted that: "While we acknowledge that management has a work plan and strategy in place to remediate some known/identified operational control deficiencies, the design of these controls is still in progress. As a general observation, the current inherent risk faced by the School District is "High" because there are significant gaps in foundational information security practices."

Areas identified during our internal audit that require attention include the need to:

- Define, document and communicate IT policies and procedures.
- Transition to a Centralized IT Governance – other organizational units in the school district make IT decisions without approval/input/oversight from IT management. Without centralized governance these "Shadow IT" decisions lead to lost control and visibility over critical and sensitive data. This increases the risk of security and regulatory non-compliance, and privacy breaches.
- Raise staff awareness and understanding of IT Security leading practices.
- Create formalized roles and responsibilities with respect to IT Security.

### **Management Response**

As a response to the Audit findings, it was determined that a Cyber Security and Risk Policy be drafted as a first step towards establishing stronger governance over IT decisions and a lowering of Cyber Risk.

Given the growing information security attack points and our vast array of devices at differing patch levels, applications, records and information stores with varying access controls, this is a first step to establishing accountability on proactive standards, controls, training and oversight.

Summary of the philosophy behind the policy statements:

- Cyber Risk is primarily carried by the Board and Executive. It is now widely believed to be one of the highest risks facing Boards of organizations.
- The Board of Education believes that it is essential to protect the digital assets of School District 62 from all cyber risks, whether internal or external, deliberate or accidental.
- The role of the Chief Information Officer (CIO) is to set IT policy & standards, direct and monitor the design and implementation of effective information security and privacy controls, and provide training to staff to build capacity and awareness of IT processes and policies in the district.
- Operational responsibility for compliance with security policy, its regulations and associated procedures and standards rest with the accountable Executive for each site/department.
- Security assurance must be balanced against functional and operational needs and budgetary constraints.

### **Feedback from the September Education Policy Meeting**

The following feedback and questions were provided on the draft policy at the Education Policy Meeting in September 2022:

1. **Training** - Who is responsible for training staff? How do we ensure ongoing training? Should this be captured in the policy, including who has responsibility/oversight for ensuring it is done?
2. **Breaches** - What is the approach/process for reporting suspected cyber security and privacy breaches?
3. **Language** - Review and clarify language on security screening for new employees and “discipline for breach”.
4. **Non-District-Managed Devices** - Board wanted to gather ideas from other districts as to how they are handling the Bring Your Own Device (BYOD) issue, especially from a privacy perspective.
5. **Surveillance of staff** - Concerns regarding staff being subject to "district surveillance" on district networks.
6. **Costs** - How will the costs associated with the implementation of this policy be brought forward as part of the process?

### **Work has been done by staff to address the questions raised by the committee:**

**Q1: Training** - Who is responsible for training staff? How do we ensure ongoing training? Should this be captured in the policy, including who has responsibility/oversight for ensuring it is done?

This has been addressed in the Policy statements and Regulations:

### **Principles that guide the security of Information and Technology (Digital Assets) at SD62:**

- Information security training is provided to all employees.

## Regulations Section 2: Responsibilities

- **Chief Information Officer is responsible for:**
  - Developing and delivering Security and Privacy Training on an ongoing basis to new and existing employees
- **Human Resources along with Hiring Supervisors are responsible for:**
  - Ensuring all new and existing employees are trained on Security and Privacy on an ongoing basis
- **Hiring of Manager, Security and Privacy:** Similar to our approach to OH&S compliance, we are hiring a Manager, Security and Privacy to help drive policy awareness, training, and implementation

**Q2: Breaches** - What is the approach/process for reporting suspected cyber security and privacy breaches?

## Regulations Section 2: Responsibilities

- **Department / Site Leadership responsibilities:**
  - Reporting suspected security and privacy incidents that affect their area of responsibility to the CIO.
  - Managing the response to security and privacy incidents that affect their areas of responsibility based on guidance from the CIO.
- **Staff responsibilities:**
  - Reporting suspected security and privacy incidents to their Supervisor.
- **Caregivers and Student responsibilities:**
  - Reporting suspected security and privacy incidents to their teacher and/or school administrators.

**Additional procedures to aid in the identification and reporting of incidents are being developed and will be communicated to staff.**

**Q3: Language** - Review and clarify language on security screening for new employees and “discipline for breach”.

### Existing SD62 [Acceptable Use of Technology Policy – B117:](#)

- **Violations of Policy:** Violations to this policy may result in privileges relating to District technology being restricted, suspended, or revoked and may result in disciplinary action.
- Violations of this policy may be reported to the appropriate law enforcement authorities and may also be subject to criminal investigations and/or criminal charges.

Having reviewed the existing policy and taking into consideration the concerns raised by the Committee, the language in the draft Cyber Risk and Security regulations has been revised and clarified:



#### Section 4: Human Resources role in Cyber Security

The role of Human Resources in cyber security is to ensure that employees, external consultants, and contractors accessing School District 62 information and information systems have been screened, understand, and accept their responsibilities for security, receive security training and that their access to information and systems is securely managed throughout their affiliation with the School District.

- Prior to employment, employee and contractor security screening is completed, and employees and contractors are informed about information security policies, regulations, procedures and associated roles and responsibilities
- Reference and criminal records checks are completed prior to hiring or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy are signed off upon hire.
- Supporting management with determining the appropriate course of action in response to identified abuse of information and technology assets.
- Security breaches or policy violations that have been reported are investigated, and action is taken where warranted.

**Q4. Non-District-Managed Devices** - Board wanted to gather ideas from other districts as to how they are handling the Bring Your Own Device (BYOD) issue, especially from a privacy perspective.

SD61 – Victoria: [Board Policy 1300 Acceptable use of Digital Technology](#) and section 5 of [Student Acceptable Use of Digital Technology Regulation](#)

**2.1 BYOD (Bring Your Own Device) refers to the practice of enabling students and staff to bring personally owned devices (such as laptops, tablets and smartphones) to school, for the sole purpose of educational use.**

2.2 Data include but are not limited to, student records, employee records, confidential, **personal**, or professional information and communications, or any other electronically stored information that passes through or is stored electronically on District Technology Resources

**2.5 Personally Owned Technology is any device that is not provided by the Board of Education, including (but not limited to) personal computers, smartphones and tablets.**

2.7 Users include (but are not limited to) students, parents, guardians, staff members, volunteers, guests, Parent Advisory Committee members, and Board of Education members given authorized access to District Technology Resources, regardless of whether access is onsite or offsite.

**3.4 Engaging in personal use is a choice users make that may involve the sacrifice of personal information. The Board of Education cannot guarantee that personal information is secure while using District Technology Resources.**

**3.8 Users who do not comply with this policy and accompanying procedures will be subject to the appropriate disciplinary actions.**

SD69 – Qualicum: 501 – [Acceptable Use of Technology\(AUP\)](#)

- **Use of technology associated with the School District, including Internet access and email, is neither private nor confidential and may be tracked. Use of such technology by any individual may be monitored or reviewed by the School District without prior notice. In the case of misuse or suspicion of misuse of the network or services, the School Board reserves the right to access any files/data on the system.**
- The District may block or remove files that are unacceptable or in violation of this Acceptable Use Policy.

SD71 – Comox Valley: [Computer and Internet Access Responsible Use Agreement](#)

- The School Board will not be held liable for any personal content housed on a BYOD device. School administrators have the authority in their role of ensuring a safe climate for all, and acting as a “judicious parent”, to take control of a student’s BYOD device if there is a significant concern and view any and all content on it (including pictures, videos, text messages, etc.).

- Parents/Guardians will be notified as soon as possible about any Agreement concerns that school administration may have about a student. Parents/Guardians who have an expectation for student privacy with a BYOD device should not allow their child to bring that BYOD device to school. The School Board is not responsible for any physical damage, loss or theft of any BYOD device.
- All Internet use and/or texting charges are the sole responsibility of the User. Users are responsible for bringing their BYOD device home each day and returning it fully charged and Users are responsible for keeping the BYOD device secure when not in use.

SD82 – Coast Mountains: [Policy 1090 Bring your own Technology \(BYOT\)](#)

POLICY Users are required to accept the following terms of use prior to connecting to the Coast Mountains network: CMSD82 is providing wireless connectivity as a service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of the CMSD82-BYOT wireless network is entirely at the risk of the user, and CMSD82 is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury or damages resulting from the use of the wireless connection.

SD34 – Abbotsford: AP417 - [Information and Communication Services.](#)

- Bring Your Own Device 3.1 The definition Bring Your Own Device (BYOD), refers to personal district network or internet-connected devices (laptops, phones, tablets, etc.), internet of things (IOT) devices and artificial intelligence (AI) devices. 3.2 Routers and wireless access points are not considered to be BYOD and are not permitted to be connected to the district's network.

SD44: North Vancouver School District has also addressed BYOD through their [Acceptable Use of Technology Agreement](#)

- Additional research was also conducted via the Office of Information Privacy Commissioner of Canada – [“Is a Bring Your Own Device \(BYOD\) Program the right choice for Your Organization?”](#)

**Q5. Surveillance of staff** - Concerns regarding staff being subject to "district surveillance" on district networks.

**While other districts have a more restrictive policy, SD62 does not conduct “snooping” on staff, PAC or parent devices. Specific conditions may require us to conduct surveillance as outlined in existing Board policy B-117 Acceptable Use of Technology:**

A system administrator will not access a staff member's history of activities except as follows:

- with the explicit permission of the staff member, or
- upon the written instruction of the Superintendent of Schools, or
- where required by law, or
- where such access is reasonably required to prevent a significant threat to personal or public safety

**Other Districts:**

SD36 – Surrey – [\(Regulation 5780.1\) Parameters for Information and Communication Technology](#)

- 6.8 The district reserves the right to monitor all user activity of district technology. 6.9 Users have limited privacy in regard to the contents of files stored on district technology. A search and investigation of any user's district computer account will be conducted if there is reasonable suspicion that the terms of this policy have been violated. This process will be managed by the district Human Resources department.

SD69 – Qualicum: 501 – [Acceptable Use of Technology\(AUP\)](#)

- Use of technology associated with the School District, including Internet access and email, is neither private nor confidential and may be tracked. Use of such technology by any individual may be monitored or reviewed by the School District without prior notice.

**Simcoe County District School Board: [EMPLOYEE ELECTRONIC MONITORING 3007](#)**

- Rationale Ontario's new law under Bill 88: Working for Workers Act, 2022, requires employers with 25 or more employees to have a written Electronic Monitoring Policy in place prior to October 11, 2022. The Simcoe County District School Board (SCDSB) is committed to providing a transparent and fair workplace for all staff. Through this Employee Electronic Monitoring Policy and its related administrative procedures memorandum (APM), the SCDSB will communicate the Board's intent to monitor its employees and provide information about the categories of information collected and how that information may be used.
- **Policy:** It is the policy of the SCDSB that the Board may monitor and may access employee electronic files, documents, records, communications and use of the Internet, at any time, to ensure the integrity of the system, safety of the workplace and compliance with Board policies and procedures.

**Q6. Costs** - How will the costs associated with the implementation of this policy be brought forward as part of the process?

The following costs will need to go to Resources Committee as part of the annual budget submission process:

- Manager, Cyber Security and Privacy
- Security Awareness Training – software and release time
- Encrypted file-sharing capability for sensitive data
- Software for log management and event correlation (SIEM/SOAR), and other technologies recommended in the internal audit report
- Periodic Vulnerability Assessments, “Ethical hacking” and Cyber maturity studies as recommended in the internal audit report
- Cyber Insurance and incident response service

**Recommendation:**

Given the required period for Notice of Motion for draft new Policy and Regulations F-325 “Cyber Risk and Security” has been served, that the Board adopt the draft new Policy and Regulations F-325 “Cyber Risk and Security”.

Respectfully submitted,

Farzaan Nusserwanji  
Chief Information Officer and  
Executive Director – Information Technology

**School District #62 (Sooke)**

|                                |   |
|--------------------------------|---|
| <b>CYBER RISK AND SECURITY</b> | No.: F-325  |
|                                | Effective:<br>Revised:<br>Reviewed: Sept. 6/22; Sept. 27/22;<br>Nov. 8/22 |

**SCHOOL BOARD POLICY****Rationale:**

The Board of Education believes that it is essential to protect the digital assets of School District 62 from all cyber risks, whether internal or external, deliberate or accidental. Therefore, it is the policy of School District 62 to provide secure access to information and technology for use by students, staff and other users in a manner that complies with related provincial legislation, district policies, regulations, and guidelines.

**Principles that guide the security of Information and Technology (Digital Assets) at SD62:**

- Information systems, data, and technologies are defined and managed as digital assets by the School District and are understood, provided, maintained, and protected as such.
- There is no such thing as absolute security – protection is balanced with utility.
- The primary goals of cybersecurity are to maintain Confidentiality, Integrity, and Availability of information.
- security controls need to be Preventative, Detective, and Responsive.
- People, Processes, and Technology are all needed to secure an information system or facility.
- Information is not modified by unauthorized persons through deliberate or careless action.
- Information is not provided to unauthorized persons through deliberate or careless action.
- Apply the “need to know” and “least privilege” principles to protect sensitive information
- Regulatory and legislative requirements (e.g. FOIPPA, Statistics Act) are met.
- Digital security governance practices are established and followed.
- Business continuity plans to respond to cyber security events are produced, maintained, and tested.
- Information security training is provided to all employees.
- All breaches of information security and suspected weaknesses must be reported and investigated.
- Access to software, hardware and 3rd party cloud services that pose a security risk may be restricted.
- Exceptions to the policy require the Executive to make recommendations to the Board.

**Related Policies and Legislation:**

- Policy B-115 – Learning Resources
- Policy B-117 – Acceptable Use of Technology
- Policy F-200 – Purchasing
- School Act
- FOIPPA – Freedom of Information Privacy Protection Act

**School District #62 (Sooke)**

|                                |   |
|--------------------------------|---|
| <b>CYBER RISK AND SECURITY</b> | No.: F-325  |
|                                | Effective:<br>Revised:<br>Reviewed: Sept. 6/22; Sept. 27/22;<br>Nov. 8/22 |

**ADMINISTRATIVE REGULATIONS**

The following administrative regulations support and further define cyber risk and security in the Sooke School District and are provided within the Cyber Risk and Security Policy.

**1. Application and Scope**

All School District 62 staff, students and vendors employed under contract, who have any involvement with digital assets, are responsible for implementing this policy and its regulations and shall have the support of the School District 62 Board which has approved the policy. This policy and its regulations cover digital assets and initiatives whether hosted by SD62 or a third party. Failure to comply with this policy may result in breaches of security, leading to the exposure of data of a confidential or sensitive nature.

**2. Responsibilities pertaining to Cyber Risk and Security**

**The Board of Education's** responsibilities:

- Board-level digital governance: setting policy, ensuring strategic alignment, risk assessment, resource management, and performance management of cyber risk and security efforts.
- Provide oversight, guidance, and direction on the cyber risk associated with digital initiatives
- Allocate funding for information and technology asset acquisition, currency, replacement, and operational support to ensure the protection of information technology assets and the provisioning of resources to ensure adequate security and privacy are maintained.
- Provide guidance on cyber risk tolerance and be ultimately accountable for cyber risk acceptance.

**District Executive** responsibilities:

- Provide direction and funding for information and technology asset acquisition, currency, replacement, and operational support to ensure the protection of information technology assets and the provisioning of resources to ensure adequate security and privacy are maintained.
- Provide oversight, guidance, and direction on the cyber risk associated with digital initiatives.
- Ensure each business or educational application, information and data system has an Accountable Executive who ensures cyber risk and security are assessed for the systems under their executive or departmental purview.
- The accountability to ensure the cyber risk assessment is conducted and associated recommendations implemented reside with the program/business owner.

**Chief Information Officer** responsibilities:

- Board's delegate for the Cyber risk assessment and security of digital assets, digital initiatives, systems infrastructure, and information contained therein, user access controls and data recovery.
- Develop administrative procedures and standards consistent with this policy and its regulations.
- Provide strategic direction and recommendations related to the security and privacy of district digital solutions, information services and technology to the Board and its committees.
- Managing information and technology legislation, including FOIPPA and the Statistics Act

- Collaborating with District Executive to develop and set policies, standards, processes, procedures, and guidelines for cyber risk and security.
- Ensure the implications of cyber risk and security are considered during strategic planning, staffing, budget, and risk management.
- Oversee and guide the security and privacy of digital transformation initiatives across the district
- Define the privacy and security posture including operational responsibility for the FOIPPA office
- Ensure Disaster Recovery plans are updated to reflect changes in assets and security configurations.
- Develop and deliver security and privacy training on an ongoing basis to new and existing employees

**Human Resources along with Hiring Supervisors** responsibilities:

- Prior to employment, employee and contractor security screening is completed, and employees and contractors are informed about information security policies, regulations, procedures and associated roles and responsibilities
- Reference and criminal records checks are completed prior to hiring or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy are signed off upon hire.
- Supporting management with determining the appropriate course of action in response to identified abuse of information and technology assets.
- Security breaches or policy violations that have been reported are investigated, and action is taken where warranted.
- Ensuring that a process is in place for the departure of employees, consultants, contractors, or temporary agency staff in relation to the retrieval of assets and reminding employees of their ongoing confidentiality responsibilities.
- If assets are not returned, follow up to attempt retrieval or seek additional remedies.
- Contractor responsibilities for information security are identified in contractual agreements.
- Ensuring all new and existing employees are trained on Security and Privacy on an ongoing basis.

**Finance / Accounts Payable/Procurement** responsibilities:

- Ensure the Chief Information Officer has been consulted during procurement and receives reports of all hardware, software, and cloud-based services to assess compliance with this policy and its regulations.
- Confirm risks related to external party access to information and information systems are assessed before accepting any acquisition of third-party software or cloud-based services
- Ensure the risks of external party access to information and information systems are identified, assessed, mitigated and managed
- Confirm security controls, service definitions, and delivery levels are identified and included in agreements with external parties before using external information and technology services

**Director, Facilities** responsibilities:

- Developing and implementing the Physical and Environmental Security Program in consultation with the Chief Information Officer.

**Internal Audit** responsibilities:

- Conduct periodic reviews of processes, controls, and compliance with this policy and its regulations.

**Department / Site Leadership** responsibilities:

- Managing the use of the assets by employees at their site or within their site or department.
- Determining access levels and ensuring all staff in their area use IT assets responsibly.
- Monitoring compliance with this policy.

- Retrieving assets from departing employees, consultants, contractors, or temporary agency staff.
- Informing staff of their information security responsibilities and providing guidelines that clearly define how these security controls are managed.
- Notifying Information Technology of systems access requirements, changes to access requirements and removal of access when it is no longer required.
- Ensuring all privileged identities are tracked and recorded with the IT department.
- Promoting a *culture* of security, creating an appropriate level of awareness of security controls among staff, relevant to their roles and responsibilities, and an appropriate level of skills to comply with these security controls.
- Creating awareness of new or updated security requirements and monitoring adherence to the organization's security policies.
- Reporting suspected security and privacy incidents that affect their area of responsibility to the CIO.
- Managing the response to security and privacy incidents that affect their areas of responsibility based on guidance from the CIO.

**Staff responsibilities:**

- Complying with School District 62 security policies, controls, standards, and procedures, and any department or school-specific security practices.
- Familiarizing themselves with security policies and reviewing them.
- Reporting suspected security and privacy incidents to their Supervisor.
- Returning technology assets when leaving the organization.
- Notifying the IT department of any loss or damage to assets.

**Caregivers and Student responsibilities:**

- Complying with School District 62 security policies, controls, standards, and procedures, and any school-specific security practices.
- Ensuring consent is provided for use of digital tools, software and cloud-based services
- Reporting suspected security and privacy incidents to their teacher and/or school administrators

### 3. Digital Asset Management

Information and information systems constitute valuable School District 62 resources. Digital asset management identifies what assets to protect, how to protect them, and how much protection is adequate.

**Identification of Digital Assets**

School District 62 departments and schools must identify and maintain an inventory of assets under their control including:

- Hardware
- Software
- Digital services including communications and cloud-based services.
- Digital information and data assets including student and staff records, database and data files, contracts and agreements, system documentation, research information, reports, user manuals, operational or support procedures, continuity plans and archived information.

**Documenting and Maintaining Asset Inventories**

School District 62 will establish and maintain an IT Asset Management program, create and maintain an inventory of important assets associated with information systems, and establish asset currency and lifecycle plans. The loss, theft or misappropriation of assets must be reported immediately to the IT Service Desk. Where the loss, theft or misappropriation involves information the Incident Response Plan will be initiated.

The IT Asset Management program must include:

### **Hardware Assets**

- Hardware components shall be subject to full lifecycle management from acquisition to disposal, including hardware acquired but not implemented, hardware in storage or retired hardware.
- All hardware including servers and end-user computing devices must be refreshed with a currency cycle of no more than 4 years or the useful life of the device (as per support policies from the manufacturer) to ensure security updates, fixes and patches can be applied and maintained.
- All hardware items, excluding low-value assets such as mouse devices, shall be uniquely named with an asset number and labelled. Vendor decals, stickers and other serial number identifiers should not be removed. Serial numbers and model numbers shall be recorded and tracked.
- IT Operations shall periodically confirm physical inventory via automated discovery tools and reconcile and document any discrepancies.
- All allocations, transfers, returns and disposals shall be tracked and documented except for low-value assets such as mouse devices.
- Lost assets shall be reported and investigated for a potential data breach.
- Service Request processes shall be used for replacements and upgrades.
- At end-of-life hardware assets will be logged and disposed of securely to protect School District 62 information.
- All student devices must be maintained at a security patch level that ensures adequate protection.
- All hardware assets including the operating system and installed software must be patched and upgraded to no more than 2 patch levels behind the latest release.
- All critical production hardware assets shall be supported by warranty or other maintenance agreements and shall be replaced before the expiry of support agreements.
- A process for recovery of hardware after notification of staff or contractor departures shall be in place.
- Hardware configurations shall be managed through configuration management processes and documented.
- Disaster Recovery plans shall be updated to reflect changes in assets and configurations.

### **Software Assets include digital communications and cloud-based services that are not hosted on-premise**

- Disaster Recovery plans shall be updated to reflect changes in assets and configurations.
- All software licensing agreements and compliance shall be actively managed.
- All software installed on School District 62 hardware is to be appropriately licensed.
- All educational software must be reviewed for conformance with curricular, inclusion and diversity objectives and for the protection of student privacy, student records management and information protection compliance.
- All non-standard software implementations shall be managed and documented through an exception process.
- All software assets including the operating system and installed software must be patched and upgraded to no more than 2 patch levels behind the latest release.
- Variations in versions of software shall be minimized.
- Installed software versions shall be supported by vendors with patches available to address vulnerabilities.
- All digital communications and cloud-based services will be governed by the third-party vendor management framework under IT oversight.



## Information and Data Assets

- Data will be treated as an asset and protected as such.
- The goals of data security include purpose limitation, fairness, lawfulness, transparency, data minimization, storage limitation, accuracy, confidentiality, integrity and accountability
- Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
- Data (student, staff, financial statements, contracts, etc.) will be protected from unauthorized access and modification.
- Data shall be backed up regularly and disaster preparedness and recovery plans will be developed to protect and recover data from outages due to system outages or security breaches such as ransomware.
- Data classification, data standards, and data definitions shall be established to ensure the consistency of the information being shared. (Refer to section: **Data and Information Classification and Retention**)
- Every data source or application system will have a defined responsible steward who will act to ensure data security, data quality, availability, accuracy and transparency following the security policies, regulations and standards
- Integration and automation of data flow between different systems shall be securely implemented.

## 4. Human Resources role in Cyber Security

The role of Human Resources in cyber security is to ensure that employees, external consultants, and contractors accessing School District 62 information and information systems have been screened, understand, and accept their responsibilities for security, receive security training and that their access to information and systems is securely managed throughout their affiliation with the School District.

- Prior to employment, employee and contractor security screening is completed, and employees and contractors are informed about information security policies, regulations, procedures and associated roles and responsibilities
- Reference and criminal records checks are completed prior to hiring or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy are signed off upon hire.
- Supporting management with determining the appropriate course of action in response to identified abuse of information and technology assets.
- Security breaches or policy violations that have been reported are investigated, and action is taken where warranted.
- Ensuring that a process is in place for the departure of employees, consultants, contractors, or temporary agency staff in relation to the retrieval of assets and reminding employees of their ongoing confidentiality responsibilities.
- Ensuring School District 62 assets are returned on termination of employment unless other arrangements are made in advance and all School District 62 information and documents have been removed.
- If assets are not returned, follow up to attempt retrieval or seek additional remedies.
- Contractor responsibilities for information security are identified in contractual agreements.
- Ensuring all new and existing employees are trained on Security and Privacy on an ongoing basis.
- Ensuring access rights to information systems are terminated on termination of employment. Any school district data associated with the account access will be made available to the supervisor.

## 5. Physical and Environmental Security

IT equipment must be protected to reduce the risks of unauthorized access, environmental threats, and hazards. Physical and environmental security ensures that School District 62 has a risk-based physical and environmental security framework to govern the design, implementation and management of facility security and access to sites and facilities.

### Physical Security

Physical security refers to the measures designed to prevent unauthorized physical access to equipment, facilities, material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft, and other covert or overt acts. SD62 will design, document and implement security controls for a facility based on an assessment of security risks to the facility and establish appropriate entry controls to restrict access to secure areas and prevent unauthorized physical access to district information and devices.

### Environmental Security

SD62 will ensure environmental security design to address the requirements to provide appropriate temperature and humidity controls, dust control, fire protection, power, and natural disaster protection necessary to ensure the continuity of operations for the School District's facilities and equipment. Digital assets in schools such as servers, switches and network devices should be adequately ventilated and free from obstruction to ensure the stability and security of systems.

## 6. Network Security Controls

A range of controls must be implemented to achieve and maintain security and reliable access and performance within School District 62 network.

Network infrastructure security controls and security management systems must be implemented for networks to ensure the protection of information and attached information systems.

School District 62 must protect network-related assets including:

- Information in transit.
- Stored information (e.g., cached content, temporary files).
- Network infrastructure.
- Network configuration information, including device configuration, access control definitions, routing information, passwords, and cryptographic keys.
- Network management information.
- Network pathways and routes and bandwidth resources.
- Network security boundaries and perimeters.
- Information system interfaces to networks.

Employees, contractors, and external consultants must not store School District 62 information on non-School District 62 owned and managed computing devices. Non-School District 62-owned computing devices must follow the BYOD expectations when connecting to the School District 62 network.

### Inappropriate Use

Any device found to be in violation of this regulation or found to be causing problems that may impair or disable the network in any way, may be subject to immediate disconnection from the network.

Attempting to circumvent security or administrative access controls for information resources is a violation of this regulation. Assisting someone else or requesting someone else to circumvent security or administrative access controls is also a violation of this regulation.

Network usage judged inappropriate includes, but is not limited to:

- Establishing unauthorized network devices, including a router, gateway, or remote access service such as wireless.
- Using network services or devices to conduct any unlawful activity.
- Using network services that, while legal, would reasonably be considered unacceptable to School District 62's practices.
- Engaging in network packet sniffing other than for network problem diagnosis.

### **Configuration Control**

To maintain the integrity of networks, all changes to network and server configuration must be managed and controlled such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse, or loss using controls such as:

- Encryption
- DMZ and network segregation
- Access controls and multi-factor authentication
- Monitoring of access
- Configuration change logs
- Configuration baselines protected by cryptographic checksums
- Regular backups

Firewall reviews must be performed at least annually by the information technology department and after any significant changes to ensure those configuration baselines reflect actual device configuration.

### **Secured path for Confidential/Sensitive information**

Secured paths must be used for transmission of personally identifiable and sensitive/confidential information transmission using controls such as:

- Data, message, or session encryption
- Encrypted email, secure file transfer systems

### **Wireless Local Area Networking**

Wireless Local Area Networks must utilize the controls specified below:

- Strong link layer encryption, such as Wi-Fi Protected Access.
- User and device network access is controlled by School District 62 authentication services.
- The use of strong, frequently changed, automatically expiring encryption keys and passwords.
- Segregation of wireless networks from wired networks using filters, firewalls, or proxies.
- Port-based access control, for example, use of 802.1x technology.

### **Management of Removable Media**

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained in the media.

## Use of Portable Storage Devices

The use of portable storage devices to store or transport information increases the risk of information compromise as these devices are easily lost, stolen or damaged, particularly when transported in public environments. Employees using portable storage devices must protect the information and information technology assets in their custody or control by ensuring it is physically secure.

## 7. Bring Your Own Device (BYOD)

School District 62 recognizes that users may choose to access SD62 District Technology Resources utilizing a personal electronic device including but not limited to computers, phones, tablets, cellular/mobile technology, internet of things (IoT) and artificial intelligence (AI) devices. Routers and wireless access points are not considered to be BYOD and are not permitted to be connected to the district's network.

By connecting to or using the District Technology Resources (e.g. Wi-Fi network, information systems) through a personally owned device, to reduce risk and ensure security, users accept a loss of personal privacy. District authorities reserve the right to audit the device and its network usage when necessary to mitigate cyber risk and ensure compliance with school and school district codes of conduct, policies, and guidelines.

Cyber Security audits and investigations are conducted on the express authority of the Superintendent of Schools.

- Under FOIPPA, if users have records on their personal devices (BYOD) SD62 authorities can request users to search those devices themselves.
- Any failure to disclose any record or an attempt to alter a record is considered an offence under the act.
- SD62 authorities can search personal devices after informing the user and getting consent.
- SD62 authorities cannot search personal devices electronically without informing the user.
- Emergency situations, written police requests, and compelling health and safety (e.g. suicide or attack threats) are exceptions that may allow SD62 authorities to collect and disclose information after engaging legal advice.

The use of personally owned devices will follow the regulations outlined in Policy B-117 Acceptable Use of Technology.

## 8. Business Information Systems

Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems (e.g. including but not limited to HR, Finance, Facilities, Payroll, Transportation and Student Information systems).

System and Security management controls should be developed, documented, and implemented by the Accountable Executive and their staff to ensure:

- Duties and areas of responsibility are segregated to reduce opportunities for unauthorized modification or misuse of information systems.
- Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system are carried out before acceptance.
- Security review and acceptance criteria are included as part of the information system development and software acquisition process.
- Security awareness, prevention and detection controls are utilized to protect information systems against malicious code.
- Records are maintained of changes to published information (audit and change logs).

- Inappropriate release of sensitive or personal information is prevented.
- Monitoring is conducted for unauthorized changes.
- Unauthorized access to networks and information systems is prevented.
- All privileged identities are tracked and recorded with the IT department.
- Audit logs recording user activities, exceptions and information security events must be produced and stored to assist in access control monitoring and future investigations.
- Secure forms of data transmission are used (e.g. encrypted email) to transfer sensitive and personally identifiable data.
- HR, Payroll, Facilities, Transportation and Finance information systems are compliant with this policy and its regulations.
- Oversight assurance and periodic review of security controls by the IT department are undertaken.

### **Online Transaction Security**

Information systems containing online transactions must have security controls commensurate with the value and classification of the information.

Security controls must be implemented to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials.
- Using digital signatures.
- Multi-factor authentication.
- Using cryptography to protect data and information.
- Establishing secure communications protocols.
- Storing online transaction details on servers within the appropriate network security zone.

### **Publicly Available Information**

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

### **Internet Site Security**

The publication, modification, or removal of information on publicly available information systems must be approved by the staff member managing the website content. Staff who are website content managers are responsible for maintaining the accuracy and integrity of published information.

## **9. Access Control**

Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by regulations that protect particular types of information (e.g. public, internal, confidential) and FOIPPA requirements. Mechanisms for access control include password management, user authentication and user permissions.

### **Access Control**

Access to information systems and services must be consistent with business needs and be based on security requirements. All privileged accounts and identities must be tracked and recorded with the IT department.

Access controls should:

- Consider both physical and logical access to assets.
- Apply the “*need to know*” and “*least privilege*” principles.
- Set default access privileges to “deny-all” before granting access.

- Require access by unique user identifiers or system process identifiers to ensure that all accesses are auditable.
- Have permissions assigned to roles rather than individual user identifiers.
- Use encryption and multi-factor authentication

### **Access Management**

There must be a formal user registration and de-registration process for granting access to all information systems in use within School District 62. It is each department's responsibility to ensure that access controls are implemented for information systems within their management purview.

### **Password Management**

The issuance of authentication credentials must be controlled through a formal management process. Individuals must be formally designated to have the authority to issue and reset passwords.

### **Review of Access Rights / Privileges**

User access rights must be reviewed at regular intervals. A formal process must be implemented for the regular review of access rights. Privileged and Administrative accounts must be registered with IT and access logs reviewed regularly.

## **10. Cyber Risk Assessment**

A cyber risk assessment will be performed at the start of all digital initiatives to ensure that cyber risk management controls are identified and considered at the start of the initiative and through the life cycle of service delivery.

The accountability to ensure the cyber risk assessment is performed remains with the program/business owner. The program/business owner will own the risks identified in the cyber risk assessment, and its disposition, and agree to establish completion dates for cyber risk management controls that are identified (ex. Consent process for students) as part of the cyber risk assessment.

The CIO or IT department representative reserve the right to identify and block hardware, software or a 3<sup>rd</sup> party cloud service from the network and notify the accountable executive if the risk is high, and/or if the program/business owner has not agreed to implement the appropriate cyber risk management controls within a reasonable timeframe.

## **11. Information Security and Privacy Breach Incident Management**

School District 62 will establish procedures and processes so that employees, external consultants, and contractors understand their roles in reporting and mitigating security events.

Information security and privacy breach events and weaknesses must be immediately reported through appropriate management channels. Employees must immediately report all suspected or actual information security events to the IT Team and requirements for handling security events must be included in contracts and service agreements.

Procedures to detect, respond and recover will be established to manage security incidents and breaches.

The types, volumes and costs of information security incidents must be quantified and monitored.

## 12. Cyber Security Assessments and Vulnerability Scans

To ensure that School District 62 security posture is continuously informed and updated, management shall conduct periodic cyber security assessments against other school districts and industry standards such as NIST or COBIT.

Management will conduct periodic vulnerability scans including “ethical hacking” to determine vulnerabilities in the information systems and physical networks.

While reviewing and accepting results from these scans, SD62 will find an optimum balance between improving security opportunities and educational and administrative requirements within the financial and resource constraints of the district.

## 13. Data and Information Classification and Retention

School District 62 will establish a data classification system that identifies public, internal, and confidential information and will utilize appropriate access and transmission controls when sharing this data internally or externally. Techniques to secure data may include encrypted email and secure file transfer and storage protocols.

SD62 will establish clear data management, records management, retention, and storage policies in support of secured data access for software hosted on-premises or via 3<sup>rd</sup> party cloud service providers.

Records Management policies and retention schedules should cover staff personal records, school records, administrative records, human resources, and financial records.

All digital communications and cloud-based services will be governed by the third-party vendor management framework under IT oversight to ensure the privacy and protection of data and records management policies are followed.

### Data and Information Classification Definitions

| Classification      | Definition  |
|---------------------|---|
| <b>Public</b>       | <ul style="list-style-type: none"> <li>Any information that may or must be made available to the public, with no legal restriction on its access or use.</li> <li>While little or no controls are required to protect the confidentiality of public data, basic security is required to ensure the integrity of district information.</li> </ul>  |
| <b>Internal</b>     | <ul style="list-style-type: none"> <li>Any information that is produced only for use by members of the school district who have a legitimate purpose to access such data.</li> <li>Internal data is designated by the data owner where appropriate.</li> <li>Any information of a sensitive nature which is intended for limited internal use only (i.e. between specific individuals or groups of staff)</li> <li>Access to limited data and information is provided by the owner(s) who created it.</li> <li>Internal data is not intended to be shared with the public and should not be shared outside of the school district without the permission of the person or group that created the data.</li> <li>Internal information requires a reasonable level of security controls with a varying degree of access control.</li> </ul> |
| <b>Confidential</b> | <ul style="list-style-type: none"> <li>Any information protected by government legislation or contract. Example: Freedom of Information and Protection of Privacy Act (FOIPPA).</li> <li>Any other information that is considered by the district as appropriate for confidential treatment.</li> <li>Any information that if made available to unauthorized parties may adversely affect individuals or the school district.</li> <li>Confidential information requires the highest level of security controls with varying degrees of access control.</li> <li>Confidential data must be protected both when it is in use and when it is being stored or transported.</li> </ul>  |

## 14. Mobile Computing

School District 62 will ensure appropriate controls are implemented to mitigate cyber risks associated with the use of portable devices including laptops, iPads, smartphones, etc.

### Information protection

The use of portable devices must be managed and controlled by the Information Technology team to mitigate the inherent *risks* of portable devices using technologies such as Mobile Device Management and Encrypted Storage to ensure that SD62 administrators can monitor, track and erase data.

The use of devices such as laptops, and mobile devices (smartphones) to access, store, or process information increases the risk of information being compromised.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

DRAFT



## Definitions:

**Accountable Executive/Program/Business Owner** – a member of the District Executive who is the owner and/or sponsor of an SD62 digital initiative, software or 3<sup>rd</sup> party cloud service. Typically, accountable for overseeing district departments or schools.

**Availability** - Information or information systems being accessible and usable on demand to support business functions.

**Bring Your Own Device (BYOD)** - refers to personal district network or internet-connected devices (laptops, phones, tablets, etc.), internet of things (IoT) devices and artificial intelligence (AI) devices. Routers and wireless access points are not considered to be BYOD and are not permitted to be connected to the district's network.

**Business Continuity Plans** - contain the recovery procedures and strategies necessary to resume critical services and are activated when standard operational procedures and responses are overwhelmed by a disruptive event

**Confidentiality** - Information is not made available or disclosed to unauthorized individuals, entities, or processes. Control - any policies, processes, practices, or other actions that may be used to modify or manage information security risk.

**Cryptography** - the discipline which embodies principles, means and methods for the transformation of data to hide its information content, and prevent its undetected modification or prevent its unauthorized use.

**Cyber Risk** - a negative event caused by a threat or opportunity to exploit a weakness in underlying technology resources, processes, or people.

**Cyber Risk Assessment** - a process that assesses the cyber risks for a digital initiative in which recommendations are provided to manage such risks. This process is defined through Digital Governance.

**Information and Data** - include but is not limited to SD62 student records, employee records, confidential, personal, or professional information and communications, or any other electronically formatted information.

**Device** - An IT Resource that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, laptops, tablets, smartphones, and cell phones.

**Digital Asset** - includes district technology resources and digital district learning resources, software information systems, 3<sup>rd</sup> party cloud services, information and data, and hardware technologies. Digital assets include but are not limited to computers, phones, tablets, cellular/mobile technology, applications, emails, servers, networks, internet services, internet access, information and data, websites and any other electronic or communication technology provided by the Sooke School District or third party that exists today or may be developed in the future.

**Digital Governance** - a subset of board governance and has five primary objectives:

- Deliver value by ensuring quality IT (Information & Technology) services to facilitate innovation in delivering education and improving the efficiency of business processes.
- Create alignment with and support integration of business, educational and administrative outcomes.
- Ensure we are optimizing the use of digital resources and promoting digital literacy.
- Monitoring the performance and value derived from digital initiatives and investments.
- Mitigating IT risks.

**Digital Initiative** - any School District 62-sponsored project or initiative that involves the use of new (procured or developed) and/or enhancements to existing information and technology.

**District Technology Resources include** - Access to the District's wired and wireless network from any location, such as schools, workplaces, home or other offsite locations, Board of Education-provisioned hardware, such as desktop computers, laptop computers, tablets and printers (and including removable and/or external storage devices), Access to the Board of Education's technical support services, and Board of Education-provisioned software and applications, including cloud-based resources.

**Information System** - A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output, and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, database administration, hardware and software which contain machine-readable records. A collection of manual and automated components that manages a specific data set or information resource.

**Integrity** - the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

**Least Privilege** - a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accidents, errors, or unauthorized use.

**Need-to-know** - a principle where access is restricted to authorized employees that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

**Packet sniffing** - a technique whereby packet data flowing across the network is detected and observed.

**Security Screening** - verification of facts about individuals related to their identity, professional credentials, previous employment, education, and skills.

**Threat** – a potential cause of an unwanted incident, which may result in harm to a system or organization.

**User** - any individual who accesses SD62 IT Resources through any electronic or communication activity with any device (whether such device is personally owned or provided by the district) and regardless of the user's physical location. Users include but are not limited to students, employees, contractors, trustees, parents, guardians, volunteers, and guests.

**Vulnerability** - weakness of an asset or control that can be exploited by one or more threats

## **Committee Information Note**

### **Education Policy Committee Meeting**

#### **November 8, 2022**

#### **Agenda Item: 6a. – Strategic Plan Quarterly Report**

---

##### **Background:**

- The Board of Education, through motion, has directed staff to bring quarterly reports on progress related to the Strategic Plan and student outcomes forward for information.
  - Quarterly (Q) reports will be tabled at meetings in November (Quarter 1 - July - September), February (Quarter 2 - October-December), May (Quarter 3 - January - March) and September (Annual).
- Under the district's Strategic Plan 2021-2025, we have developed a comprehensive process of charting accountability that links strategic plan outcomes, the operational plans and the Ministry of Education's student success metric report: the Framework for Enhancing Student Learning (FESL).
- The [Annual Report](#) was submitted to the Board of Education at the September 2022 Board Meeting. A link to the report has been provided to the Ministry of Education.
- Annually the district takes the direction of the Board through the Strategic Plan and develops annual operational plans to assist in achieving the goals and objectives of the Strategic Plan. The [2022/23 Operational Plan](#) builds on the [2021-22 Operational Plan](#).
- The [\(FESL\) report](#) is submitted to the Ministry of Education annually on Sept 30. The report features data on SD62 student success:
  - Reading, writing and numeracy
  - Grade-to-grade transitions
  - Graduation assessments
  - Six-year and eight-year completion rates
  - Early development
  - Student satisfaction, including postsecondary and career preparation
  - Success metrics for all students, including those with unique needs, such as Indigenous ancestry, English Language Learners.

##### **Q1 Progress on the 2022-23 Operational Plan**

- The Q1 Report (Appendix 1) contains updates on each item contained in the 2022-23 Operational Plan under the headings of Learning, Engagement and Growth.
  - There are fourteen (14) items under Learning, eleven (11) under Engagement and twelve (12) under Growth.
  - Some items have multiple connections to the strategic plan. For instance, the Engagement goal initiative to develop Board/Authority Authorized (BAA) courses for the Indigenous Graduation credit required for secondary graduation connects with four elements of the strategic plan: Learning Objective 1 Provide opportunities for learners to understand, respect and appreciate diversity and inclusion. Learning Objective 2 Provide opportunities for learners to develop critical and creative thinking skills. Learning 4

Enhance student voice and choice and Engagement Objective 2. To further the goals<sup>28</sup> of the Na'tsa'maht agreement following the objectives of 'One Mind' and 'One Spirit'.

- As much of this work has only just got underway, many of the operational plan items up to September 30, 2022, were building their teams and planning the year's work. Some of the work began in July by those staff on 12-month contracts.
- Some items such as the work on Healthy Schools, Healthy People, are a continuation of work begin in previous years.
- Other items are brand new such as the Student Affordability Fund which is one-year funding from the government to be distributed by the school district on projects that support families with the rising costs from inflation.

Motion Requested: That the Education Policy Committee of School District 62 (Sooke) receive the Q1 Report at the Education Policy Committee meeting of November 8, 2022.

Submitted with Respect,  
Scott Stinson, Superintendent

# Quarterly Reporting 2022-23

# Q1



# STRATEGIC PLAN

2021-2025





# Operational Plan 2022-23

## Quarter 1 Update

### Introduction

The district is committed to regular reporting in relation to its [Strategic Plan](#) and in alignment with the [Framework for Enhancing Student Learning \(FESL\)](#).

The Board of Education, through motion, has directed staff to bring quarterly reports on progress related to the Strategic Plan and student outcomes, forward for information. The district accountability process links strategic plan outcomes and Ministry of Education student success metric reporting through a continuous improvement lens.

Data and evidence from a variety of sources become available at various times throughout the school year and are reported to the Board at key intervals. Quarterly reports are utilized as the base from which the Board's [annual report](#) will be completed.

### Contents

Updates on [Operational Plan 2022-23](#) items:

- Updates on Operational Plans for **Learning**
- Updates on Operational Plans for **Engagement**
- Updates on Operational Plans for **Growth**

### Updates on Operational Plans for Learning

The strategic priority for learning in the 2021-2025 strategic plan is to: **Develop and support learners who are creative, critical and social thinkers with the capacity to be educated citizens**



There are 4 objectives within this:

- **Learning Objective 1.** Provide opportunities for learners to understand, respect and appreciate diversity and inclusion.
- **Learning Objective 2.** Provide opportunities for learners to develop critical and creative thinking skills.
- **Learning Objective 3.** Ensure our learning environments are safe, accessible and welcoming.
- **Learning Objective 4.** Enhance student voice and choice.

There are fourteen (14) items in the Operational Plan for 2022-2023 to ensure that progress is made to the strategic priority for learning. An update for each of the 14 items is provided below:

## **Operational Plan 2022-23 Strategy - Support the collaborative work of Inclusive Education Services (IES) with all District Principals (L1).**

### **Quarter 1 Update**

Initial meetings with District Principals have been held to begin dialogue on collaborative work and create a shared understanding of the beliefs and values that guide practice within IES. There has been a restructuring of District and



School-Based PVP meetings to support collaboration and across department initiatives.

### Strategic Plan Link

This collaborative work will help feed into opportunities for learners to understand, respect and appreciate diversity and inclusion.

## Operational Plan 2022-23 Strategy - Develop a Curriculum Operations Plan with a focus on: K-12 Literacy, including a focus on building and strengthening relationships across all levels (L1, L2). Assessment, evaluation, and reporting policy (G3).

### Quarter 1 Update

The Curriculum Operations plan has been finalized based on discussions held in Spring 2022 and reflects the work for the current school year. Key updates include:

#### 1. **K-3 Literacy Intervention**

The K-3 Literacy Intervention Plan has been launched. All elementary schools are staffed with Literacy Intervention Teachers (LIT). LIT staff have met and engaged in training. LIT staff have completed the pre-assessment to establish baselines of their student's literacy levels. LIT staff are engaging in the K-3 Literacy Intervention working with classroom teachers and students.

#### 2. **Literacy Intervention (Intermediate, Middle and Secondary).**

The Intervention plan has been finalized for Intermediate students and those at Middle and Secondary schools. Meeting and training schedules for interested teachers have been established. The project is set to launch in November 2022.

#### 3. **Assessment, Evaluation and Reporting.**

The reporting pilot has concluded as of June 2022. 2022-23 Reporting guidelines have been brought through the CSL A5 committee. The system has been informed as to expectations for the current school year as well as for 2023-24. Training is being planned for teachers needed support to transition to the reporting order expectations for 2023-24. The district is

engaging in a proof-of-concept pilot for [SPACES EDU](#). This a digital portfolio and reporting tool in use in 29 other districts. Based on results it will be determined if this will be funded K-12 in 2023-24. Procurement of Spaces.edu to support Communicating Student Learning (CSL) reporting has been completed. Implementation is underway.

### Strategic Plan Link

This initiative provides opportunities for learners to understand, respect and appreciate diversity and inclusion and provides opportunities for learners to develop critical and creative thinking skills. In addition, it embraces digital technologies and help to manage the increasing complexity of the district education system by leveraging the strategic use of resources.

## Operational Plan 2022-23 Strategy - Continue to build and expand ways to improve and measure students' creative, critical and social thinking (L2)

### Quarter 1 Update

Key components of the finalized Curriculum Operations plan focus on this area. Key updates include:

1. Advocates for Curriculum Transformation: These are volunteer teacher positions in all schools that have a focus on embedding teacher-leaders in schools. Focus is on developing organic conversations, staff partnerships and working groups to explore and implement all aspects of the "new" curriculum including creative and critical thinking.
2. Finalization and launch of the Library Learning Commons (LLC)  
Philosophy: Emerged through Program Review. Finalized with stakeholder participation. Presented to Education Policy Committee. Will enhance the LLC as a place of student learning and engagement with opportunities to further develop creative, critical and social thinking.

The aim of this work is to:

- See capacity increased among teachers to develop skills among students.
- See improvement in student ability in key areas.

### Strategic Plan Link

This initiative provides opportunities for learners to develop critical and creative thinking skills.

**Operational Plan 2022-23 Strategy - Develop a learner profile tool for students with Indigenous ancestry, with the potential to expand to all students to support their academic success as identified in through the Equity Scan work (L2, E2).**

### Quarter 1 Update

The team to undertake this work has been established and planning is underway. Indigenous Information System and associated data dashboards approved. Implementation in progress. Collaborative process between NIE (Na'tsa'maht Indigenous Education) and I.T. to procure app and associated dashboard has been established with a project plan.

### Strategic Plan Link

This initiative helps provide opportunities for learners to develop critical and creative thinking skills. It also furthers the goals of the Na'tsa'maht agreement following the objectives of 'One Mind' and 'One Spirit.'

**Operational Plan 2022-23 Strategy - Develop training: for the Leadership Team that includes labour relations, collective agreements, conflict management; and for schools develop training in labour relations and human resource practices. Staff training in these areas will provide ongoing support for the work of the department (L2).**

### Quarter 1 Update

First Leadership Team training session was conducted on August 30th. Additional sessions are under development. By the end of the school year, the intent is to have a curriculum of development opportunities being implemented.

### Strategic Plan Link

This initiative provides opportunities for learners, in this case staff, to develop critical and creative thinking skills.

## **Operational Plan 2022-23 Strategy - Begin the implementation of the Middle School Philosophy including the development of consistent timetable principles across all middle schools (L1, L2, L3, L4).**

### Quarter 1 Update

Sooke's Middle School Philosophy has been reviewed, new PVP at this level have received the documentation. The Middle School Philosophy team is ready to focus on the development of consistent timetable principles during Q2.

### Strategic Plan Link

The implementation of the Middle School Philosophy works to meet all four objectives in the learning objectives of the strategic plan: Provide opportunities for learners to understand, respect and appreciate diversity and inclusion. Provide opportunities for learners to develop critical and creative thinking skills. Ensure our learning environments are safe, accessible and welcoming. Enhance student choice and voice.

## **Operational Plan 2022-23 Strategy - Explore ways to provide blended learning at the elementary level and expand at the middle school level (L3 and L4).**

## Quarter 1 Update

A district middle school, blended learning team has been established and has met twice to review progress and program, establish norms and processes for intake and transition between programs. Best practices, resources and planning for 2023-24 middle school blended programming is currently underway.

Elementary blended learning program discussions will begin in early November.

## Strategic Plan Link

This project supports objectives 3 and 4 of the objectives for learning: ensuring our learning environments are safe, accessible and welcoming; and enhancing student choice and voice.

# Operational Plan 2022-23 Strategy - Lead the consultation and expenditure of the Student and Family Affordability Fund (L3).

## Quarter 1 Update

The Minister of Education and Child Care, Jennifer Whiteside, announced the introduction of the Student and Family Affordability Fund. The \$60 million provincial fund is intended to support students and families who are struggling with rising costs due to global inflation. The district has received an allocation of \$1,251,529. Work has been undertaken to consider ways to distribute. Per Ministry of Education and Child Care direction, the district has engaged Indigenous partners, the Sooke Parents Education Advisory Council (SPEAC) and other stakeholders to inform the development of the action plan. Consultations focused on developing an understanding of unique needs, prioritization of needs, barriers and stigma related concerns.

A three-tiered approach has been developed to distribute the funds.

Tier 1 is District-based initiatives. These initiatives are organized and implemented at the district level in consultation with district stakeholders and include selected educational program fee relief at the elementary, middle, and secondary school level; expansion and development of existing and new school food programs; expansion and development of partnerships with third party community partners.

Tier 2 is School Based Initiatives. These initiatives are organized and implemented at the school level in consultation with local school stakeholders.

Initiatives will focus on additional efforts to address food security, school supply costs, additional fee relief, access to clothing and equipment required for meaningful participation in school-based programs and activities.

Tier 3 is Specialized Initiatives. These initiatives are organized and implemented at the school and district level by specialized staff including our Safe and Healthy Schools team, in particular our team of School Based Social Workers. Initiatives will focus on additional efforts to address food security, school supply costs, additional fee relief, access to clothing and equipment required for meaningful participation in school-based programs and activities by those students and families most in need.

### [Strategic Plan Link](#)

This work enhances our learning environments to be safe, accessible and welcoming.

## **Operational Plan 2022-23 Strategy - Undertake a system scan of IES services, specifically as it relates to supporting students with challenging behaviours (L3).**

### [Quarter 1 Update](#)

Full system scan of IES was done through a facilitated NID with the district IES team. This included a reflective look at changes to the system over time, roles that are currently within the department, and visions for moving forward. Meetings have been reinstated with school PVP specific to challenging presentation of student behaviour across the levels. IES leadership team began reviewing current resources in comparison to student needs to determine areas for refinement.

### [Strategic Plan Link](#)

This work helps ensure that our learning environments are safe, accessible and welcoming.

## **Operational Plan 2022-23 Strategy - Support our schools to be safe places by deepening system practices and processes to deal with the increased complexity of students and connecting schools to CIRT and VTRA processes (L3).**

### **Quarter 1 Update**

District training for CIRT has been developed and planned for a November 7th implementation. The focus will be to introduce school-based teams to the rationale, goals, and processes for a CIRT. The District CIRT members have also been extended to be inclusive of different support roles. Training has been planned specifically to support this team in a district response. Initial discussions have started to update the VTRA process and support schools in their practices.

### **Strategic Plan Link**

This work helps ensure that our learning environments are safe, accessible and welcoming.

## **Operational Plan 2022-23 Strategy - Implement learning hubs at secondary schools to enhance online learning options (L4).**

### **Quarter 1 Update**

The team to undertake the work has been established and planning is underway. Initial meeting with secondary principals, Principal of Online Learning has been held, Terms of Reference and target timelines for implementation stages have both been established. Next meeting is in early November.

### **Strategic Plan Link**

This project builds the district's ability to enhance student choice.

## **Operational Plan 2022-23 Strategy - As part of the Alternate Education portfolio: Implement and assess the “Take A Hike” program (L4).**

### **Quarter 1 Update**

The program has launched with initially sixteen (16) students and has stabilized at fifteen (15) actively-engaged students who attend every class. Initial feedback from students and staff is that program is changing lives for the youth involved.

Associate Superintendent Block attended a community launch event hosted by the Take A Hike Foundation at BoulderHouse Climbing Academy where he connected with community supports, philanthropists and politicians who were there to learn and celebrate the launch of the program in Sooke as well as hear a general overview of Take a Hike and the potential to extend the program.

### **Strategic Plan Link**

This project builds the district’s ability to enhance student choice.

## **Operational Plan 2022-23 Strategy - As part of the Alternate Education portfolio: Explore a revised vision for the Milnes Landing Alternative programming (L4).**

### **Quarter 1 Update**

The team to undertake the work has been established and planning is underway. Initial meeting with Edward Milne Community School (EMCS) PVP has been held. Terms of Reference and target timelines for implementation stages have both been established. Next meeting is in early November. Meeting with Secretary-Treasurer and actions are underway looking for suitable commercial properties in Sooke.

### **Strategic Plan Link**

This project builds the district’s ability to enhance student choice.



## **Operational Plan 2022-23 Strategy - As part of the Alternate Education portfolio: Develop a program vision for implementation at the Westshore Post-Secondary that compliments the direction of the facility (L4).**

### **Quarter 1 Update**

Executive teams from the school district and Royal Roads University met to discuss collaboration and programming possibilities the upcoming post-secondary project being built in Langford.

In addition, Associate Superintendent Block met with the Special Projects Leader at Camosun College to discuss programming intentions and needs for both the college and the school district on the Westshore.

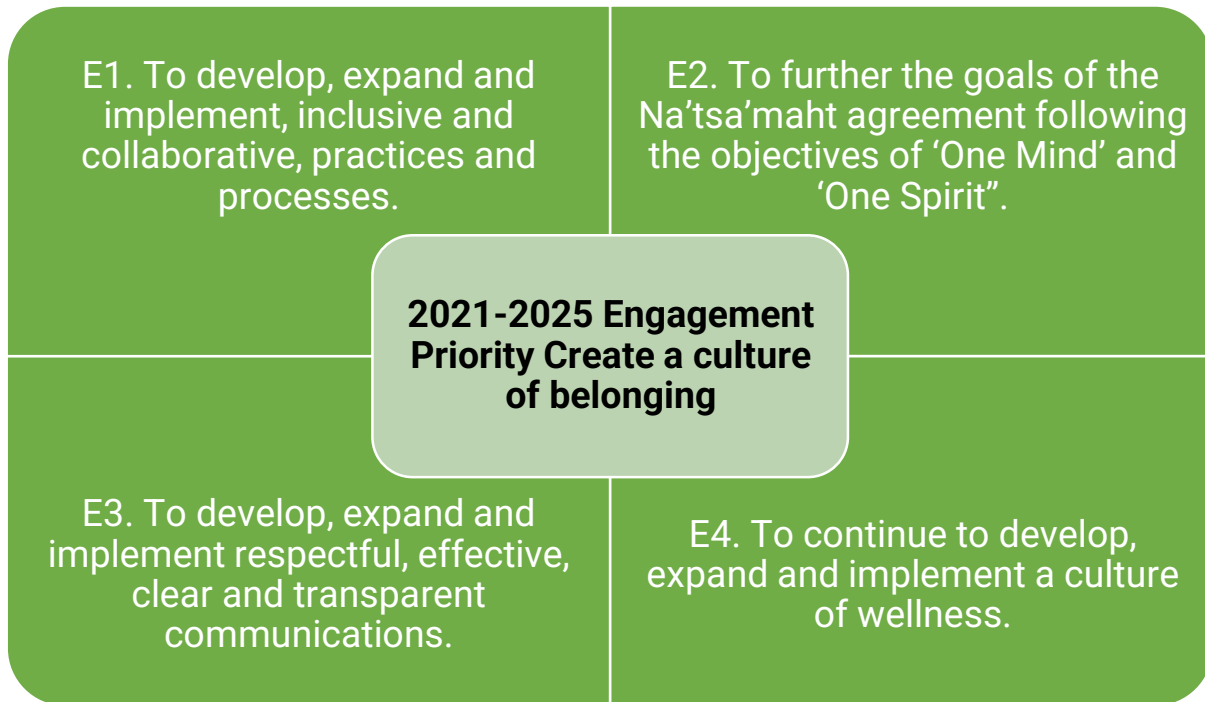
### **Strategic Plan Link**

This project builds the district's ability to enhance student choice.

## Updates on Operational Plans for Engagement

The strategic priority for engagement in the strategic plan is to:

Create a culture of belonging.



There are 4 Objectives within this:

- **Engagement Objective 1.** To develop, expand and implement, inclusive and collaborative, practices and processes.
- **Engagement Objective 2.** To further the goals of the Na'tsa'maht agreement following the objectives of 'One Mind' and 'One Spirit'.
- **Engagement Objective 3.** To develop, expand and implement respectful, effective, clear and transparent communications.
- **Engagement Objective 4.** To continue to develop, expand and implement a culture of wellness.

There are eleven (11) items in the Operational Plan for 2022-2023 to ensure that progress is made to the strategic priority for engagement. An update for each of the eleven (11) items is provided below:

## **Operational Plan 2022-23 Strategy - Distribute the process of school staffing to create shared accountability amongst the Associate Superintendents (E1).**

### **Quarter 1 Update**

Meetings have been held with Associate Superintendent Strange and District Principal of Curriculum regarding distribution of teacher-librarian staffing. They discussed the possibilities and limitations of the SAS system and the elements of the Collective Agreement that are non-negotiable as they begin to consider a variety of ways to distribute the teacher-librarian staffing. Timelines and a series of meetings have been planned to co-develop the model for 2023-2024.

Meetings with Associate Superintendent Braniff, District Principals White and Brookes regarding the distribution of inclusive education and SAFE schools staffing. They discussed the possibilities and limitations of the SAS system and the elements of the Collective Agreement that are non-negotiable as they begin to consider a variety of ways to distribute the teacher staffing. Timelines and a series of meetings have been planned to co-develop the model for 2023-2024.

### **Strategic Plan Link**

This project helps the district develop, expand and implement inclusive and collaborative practices and processes.

## **Develop and provide protocols and training for system leaders on how to receive and support claims of sexual assault and sexual harassment (E1).**

### **Quarter 1 Update**

Reviewed resources used in other BC schools to provide a foundational understanding for system leaders. Began planning develop an implementation strategy for protocols and training across the leadership team.

### **Strategic Plan Link**

This project helps the district develop, expand and implement inclusive and collaborative practices and processes.

**Operational Plan 2022-23 Strategy - Extend and implement work on recruitment and onboarding model, supported by digital processes and resources, and plan to implement training modules for recruitment that can be undertaken by the Leadership Team (E1).**

**Quarter 1 Update**

Developed project plan and agreed upon the Statement of Work. Kick-off meeting with cross-functional SD62 team and PowerSchool representatives is scheduled for November 10th.

**Strategic Plan Link**

This work will help the district to develop, expand and implement inclusive and collaborative practices and processes.

**Operational Plan 2022-23 Strategy - Begin the Implementation of the revised Na'tsa'maht Agreement (E1) and undertake to report to the Board of Education biannually on progress with the Na'tsa'maht agreement (E2).**

**Quarter 1 Update**

Host facilitate and celebrate in the Na'tsa'maht Signing Ceremony in conjunction with the national Truth and Reconciliation Events district wide at school sites and work sites.

NIE Council had initial meeting co-developing the Terms of Reference sharing the budget and staffing plan and reviewing NIE's 2022-23 operational plan.

**Strategic Plan Link**

This project furthers the goals of the Na'tsa'maht agreement following the objectives of 'One Mind' and 'One Spirit.'

## **Operational Plan 2022-23 Strategy - Develop Board/Authority Authorized (BAA) courses for the Indigenous Graduation credit required for secondary graduation (L1, L2, L4 E2).**

### **Quarter 1 Update**

Effective the 2023/24 school year, all students working toward a B.C. Certificate of Graduation (“Dogwood Diploma”), in English or French, must successfully complete at least four (4) credits in Indigenous-focused coursework. To kick off the work, Superintendent Block met with the Curriculum Team and Na’tsa’maht Indigenous Education (NIE) to discuss and plan the events and activities to support the initiative. Secondary schools have been informed of events and opportunities for feedback and input to the development of potential courses.

Reviewed BAA courses and process for development and approval with secondary school administrators in anticipation of locally developed courses.

### **Strategic Plan Link**

This project works to advance several operational objectives: to provide opportunities for learners to understand, respect and appreciate diversity and inclusion; to provide opportunities for learners to develop critical and creative thinking skills; to enhance student choice and voice; to further the goals of the Na’tsa’maht agreement following the objectives of ‘One Mind’ and ‘One Spirit.’

## **Operational Plan 2022-23 Strategy - Style Guide and Brand Guide; (2) Communications Plan; (3) Annual Event Plan and Targets (4) Clear delegation of Communication responsibilities (E3).**

### **Quarter 1 Update**

Several key strategic communications guides are now complete:

1. Style Guide and Brand Guidelines are completed.
2. Communications Plan is complete.
3. A schedule of events and media output was completed in Q1.
4. Details of communication responsibilities are contained in the Communications Plan.
5. Media Protocols for Staff and Schools

6. Crisis Communications Plan
7. Guideline for Responding to Inappropriate Correspondence

### **Strategic Plan Link**

This work helps the district develop, expand and implement respectful, effective, clear and transparent communications.

## **Operational Plan 2022-23 Strategy - Provide a system of attendance support, disability management which are supported through data on dashboards (E4).**

### **Quarter 1 Update**

The project team for this work was established in Quarter 1. The current focus is to develop robust data and reporting to fully understand the current state of staff absenteeism across all employee groups.

### **Strategic Plan Link**

This work helps to develop, expand and implement a culture of wellness.

## **Operational Plan 2022-23 Strategy - Explore and implement a revised Healthy Schools Healthy People (HSHP) framework (E4).**

### **Quarter 1 Update**

The 2021-23 HSHP Framework is in its last year of implementation. Key Updates include:

1. 2022-23 HSHP focus established based on progress in the framework through to June 2022.  
  
2022-23 goals set and strategies finalized; 2022-23 plan shared with system leaders. Implementation is ongoing.
2. Expansion of Physical Literacy mentorship project in partnership with PISE (Pacific Institute for Sport Education).

3. Establishment of school-based Health Champs and SOGI reps in all schools.
4. Establishment of district Sexual Health Education Coordinator to support instruction related to topics such as maturation, healthy relationships. Informed consent etc.
5. Capital partnerships established with members of The Village Initiative (TVI). Partners have committed to future capital opportunities to develop shared space in new school buildings.
6. TVI partners have joined the effort in actioning the Student and Family Affordability Fund.

This year will also end the current HSHP Framework. A new Framework for 2023-25 will be developed in time for the spring budget process.

### **Strategic Plan Link**

This work helps to develop, expand and implement a culture of wellness.

## **Operational Plan 2022-23 Strategy - Develop and implement a learning series for leadership on cultivating resilience (Onward) (E4).**

### **Quarter 1 Update**

Undertook initial Onward training with the Leadership Team focusing on Aptitudes and Interests and Core Values.

### **Strategic Plan Link**

This work helps to develop, expand and implement a culture of wellness.

## **Operational Plan 2022-23 Strategy - Strengthen District connections and presence in schools (E4).**

### **Quarter 1 Update**

Set aside time each week to focus specifically on building district connections and presence in schools.

### **Strategic Plan Link**

This work helps to develop, expand and implement a culture of wellness and feeds into the overall engagement Objective: to create a culture of belonging.

## **Operational Plan 2022-23 Strategy - Develop a process and implementation plan for performance management and growth in alignment with the HR Operations Plan (E1).**

### **Quarter 1 Update**

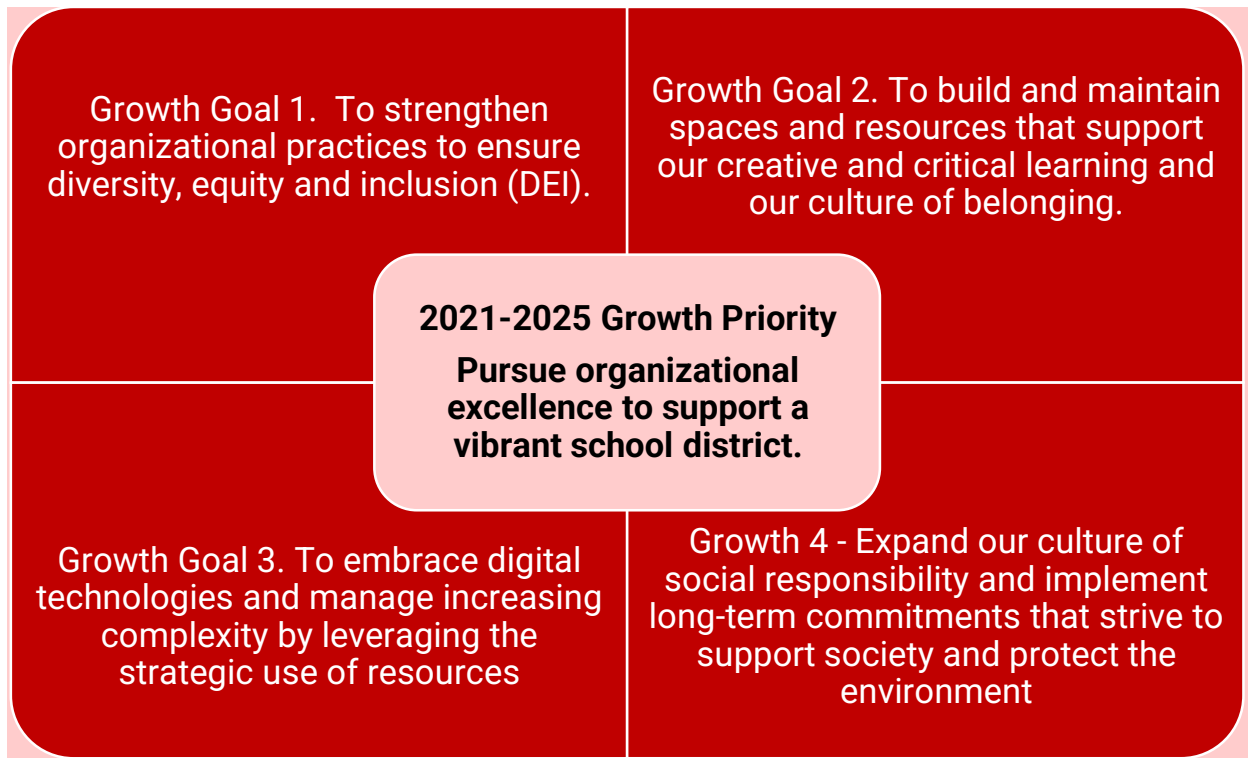
This item was deferred to a future time.



## Updates on Operational Plans for Growth

The strategic priority for growth in the strategic plan is to:

**Pursue organizational excellence to support a vibrant school district.**



There are 4 Objectives within this:

- **Growth Objective 1.** To strengthen organizational practices to ensure diversity, equity and inclusion (DEI).
- **Growth Objective 2.** To build and maintain spaces and resources that support our creative and critical learning and our culture of belonging.
- **Growth Objective 3.** To embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.
- **Growth Objective 4.** Expand our culture of social responsibility and implement long-term commitments that strive to support society and protect the environment.

There are twelve (12) items in the Operational Plan for 2022-2023 to ensure that progress is made to the strategic priority for growth. An update for each of the twelve (12) items is provided below:

## **Operational Plan 2022-23 Strategy - Use the Employment Equity Survey results to develop an action plan connected to policy development and equity hiring practices and processes (G1).**

### **Quarter 1 Update**

The Employment Equity team has met twice so far in the 2022/23 school year to review Employment Equity survey results and begin to uncover themes within the data to inform future action planning.

### **Strategic Plan Link**

This operational item works to strengthen organizational practices to ensure equity, diversity and inclusion.

## **Operational Plan 2022-23 Strategy - Develop policy related to Business Continuity Planning (BCP) and Digital Governance (G2).**

### **Quarter 1 Update**

Work on drafting policies for Business Continuity Planning and Digital Governance is underway. A refresh of BCP plan in progress.

### **Strategic Plan Link**

This item feeds into the operational item to build and maintain spaces and resources that support our creative and critical learning, and our culture of belonging.

## **Operational Plan 2022-23 Strategy - Use the 2022 Design Guidelines for Capital Construction to develop District Universal Standards that will be systematically applied to all building design and construction (G2).**

### **Quarter 1 Update**

Team established with initial plan developed to align design guidelines to district standards to technical specifications for use in future minor and major capital projects. First stage to connect guidelines to district standards.

### **Strategic Plan Link**

This item feeds into the operational item to build and maintain spaces and resources that support our creative and critical learning, and our culture of belonging.

## **Operational Plan 2022-23 Strategy - Update the Long-Range Facilities Plan (LRFP) including enrolment forecasts (G2).**

### **Quarter 1 Update**

Team established with previous LRFP procurement document being updated for issuance by Nov 30, 2022. The intent is to obtain the long-range enrolment methodology for use by staff in years in which the LRFP isn't updated.

### **Strategic Plan Link**

This item feeds into the operational item to build and maintain spaces and resources that support our creative and critical learning, and our culture of belonging.

## **Operational Plan 2022-23 Strategy - Explore the focus of I.T. as it relates to digital literacy across educational departments (learning) (G3)**

### **Quarter 1 Update**

Vision clarified and planning underway

### **Strategic Plan Link**

This operational item feeds into the organizational maturity required as the organization grows rapidly: embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - Implement the Program Review recommendations specific to finance, facilities, and transportation (G3).**

### **Quarter 1 Update**

Recommendations have been provided to individual departments for consideration prior to implementation. A work plan, including timelines to be established by Dec 31, 2022.

### **Strategic Plan Link**

This operational item feeds into the organizational maturity required as the organization grows rapidly: embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - Build a financial operating framework from an inflation-fighting financial review (G3)**

### **Quarter 1 Update**

Team established with initial planning underway involving the proposed approach to quantify inflationary pressures, develop potential structural solutions and recommendations. Framework to be developed by Jan 31, 2023, for use in the budget development process for the 2023-24 school year.

### **Strategic Plan Link**

This operational item feeds into the organizational maturity required as the organization grows rapidly: embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - Establish a Cyber Risk and Security policy and begin implementation (G3).**

### **Quarter 1 Update**

Revised policy draft will be presented to the Education Policy Committee in November. Hiring of Manager, Cyber Security and Privacy in progress.

### **Strategic Plan Link**

This operational item feeds into the organizational maturity required as the organization grows rapidly: embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - Develop a clear vision (including a clear rationale) for digital solutions in the district, which would be supported by rebranding the Information Technology (I.T.) Department to Digital Transformation Services (G3).**

### **Quarter 1 Update**

The proposed vision was presented to the District Executive and District Leadership Team. There was overwhelming support for the vision, rebranding IT to Digital Solutions and the establishment of five (5) core services under this umbrella. Development of supporting financial and staffing model in progress.

### **Strategic Plan Link**

This operational item feeds into the organizational maturity required as the organization grows rapidly: embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - Develop recommendations for digital integration through an agreed upon oversight process (governance) (L1, L2, E3, G1, G3).**

### **Quarter 1 Update**

Team established and work on developing a governance model in progress.

### **Strategic Plan Link**

This item feeds into several layers of the strategic plan: recommendations regarding data integration and governance will create a model to ensure that the district provides opportunities for learners to understand, respect and appreciate diversity and inclusion as well as providing opportunities for learners to develop critical and creative thinking skills. The process will help to develop, expand and implement respectful, effective, clear and transparent communications. In addition, the outcome will strengthen organizational practices to ensure equity, diversity and inclusion and embrace digital technologies and manage increasing complexity by leveraging the strategic use of resources.

## **Operational Plan 2022-23 Strategy - As part of transportation safety, implement enhanced safety recommendations (G4, L3).**

### **Quarter 1 Update**

In Q1, the team to work on this project was established with initial conversations centered around the viability of the existing transportation operating system and the potential to move to another system. Further planning to include reinstating the transportation safety committee and reviewing previously outstanding recommendations.

### **Strategic Plan Link**

This item meets both the objective to expand our culture of social responsibility and implement long-term commitments that strive to support society and protect the environment; it also works to ensure our learning environments are safe, accessible and welcoming.

## **Operational Plan 2022-23 Strategy - Develop a process to explore and act upon issues of diversity, equity, inclusion and anti-racism (G4).**

### **Quarter 1 Update**

Began the initial exploration of a system audit, internal and/or external, to support diversity, equity and inclusion. Met with a lead consultant to discuss the scope and timing of a possible organizational audit of current practice towards diversity, equity, inclusion (DEI) and anti-racism in the district. Connected this DEI direction to the work already underway through HR to provide meaningful alignment throughout the district.

### **Strategic Plan Link**

This item feeds into the growth objective to expand our culture of social responsibility and implement long-term commitments that strive to support society and protect the environment.



**Committee Info Note**  
**Education-Policy Committee Meeting**  
**November 8, 2022**  
**Agenda Item 6b: Update - Student and Family Affordability**  
**Fund Action Plan**

---

## **PURPOSE**

To provide the committee an update on the Sooke School District School and Family Affordability Fund Action Plan.

## **BACKGROUND**

- On Monday, August 29 the Minister of Education and Child Care, Jennifer Whiteside, announced the introduction of the Student and Family Affordability Fund.
- The \$60 million provincial fund is intended to support students and families who are struggling with rising costs due to global inflation.
- The fund is intended to:
  - Improve students' access to nutritional food/meals, before, during and after the school day.
  - Directly offset costs to parents, guardians, and students, such as school supplies or other cost pressures they are facing using existing mechanisms such as hardship policies.
- Will support school food programs and the costs of school supplies as key areas of support.
- The funding is provided on a one-time basis for the 2022-2023 school year and is not intended be structural or carried over to subsequent school years.

## **CONTEXT**

- The district has received an allocation of \$1,251,529.
- The fund requirements include:
  - consultation with local Indigenous rightsholders, to determine any unique needs for Indigenous learner, District Parent Advisory Councils (SPEAC), and "equity-deserving" communities to ensure the unique needs of all diverse student populations are met.
  - using the funds in as flexible, private and stigma free manner as possible.
- Spending descriptors include:
  - Spending on Food Security
    - Spending by the district on Food Security should be in addition to any planned or budgeted spending on food and meals programs.
    - Districts are encouraged to use healthy, local and/or B.C. food where possible and to utilize existing processes and providers (including not-for-profits).
    - Funding can be spent to:
      - Increase nutritional opportunities for students throughout the day
      - Provide nutritional food and meal support to additional students.
      - Provide additional food and meal supports to students with dependent children where appropriate Spending on Family Assistance.
  - Spending on Family Assistance
    - Spending by the district must directly offset costs for parents, guardians, and students and be additional to any planned or budgeted spending for hardship or family supports.
    - Funding use includes, but is not limited to:



- Providing basic school supplies that might otherwise be purchased by parents, guardians, and students (e.g., pens, paper).
- Waiving education-related fees (e.g., additional supplies for shop, culinary and craft classes, workbooks, camps, field trips, relevant cultural events, other student society meetings including those related to equity, diversity, and inclusion, and instrument and equipment fees or other fees charged by school districts).
- Supporting with clothing/footwear required for school sports and other school activities.

## **PROGRESS UPDATE**

- The District has completed its consultations with its partners and has developed its Student and Affordability Fund Action Plan.
- The Plan is finalized and has been shared at the October 2022 Education-Policy Committee, Resources Committee, and SPEAC meetings.
- The Plan has been published to our external school district website.
- Implementation Action to date:
  - Middle and Secondary Schools are working with the Finance Department to action specific fee refunds.
  - Schools have been allocated funds for local planning and are completing consultations with their school communities. Once completed they are being submitted to the district for approval.
  - The district has entered into several agreements with community partners that will be actioning funding in support of SD62 students and families and funds are being distributed as of this report. These partners include the Sooke Family Resource Society, BGC Southern Vancouver Island, Thrive Social Services Society, Sooke Food Bank, Goldstream Food Bank, Salvation Army, Westshore Parks and Recreation, and Food Share Network.
  - Funds have been allocated to Na'tsa'maht Indigenous Education Department to directly support local First Nations and Metis community partners over and above support through school-based plans.

Respectfully submitted,

Dave Strange  
Associate Superintendent



# Student and Family Affordability Fund: 2022-23 Action Plan



1



# Working Together to Support Students and Families

2

2



## Current Context

Minister of Education and Child Care, Jennifer Whiteside announced the introduction of the Student and Family Affordability Fund. The \$60 million provincial fund is intended to support students and families who are struggling with rising costs due to global inflation. The district has received an allocation of \$1,251,529. The funding is provided on a one-time basis for use during the 2022-2023 school year.

The fund requirements include:

- Consultation with local Indigenous rightsholders, to determine any unique needs for Indigenous learner, District Parent Advisory Councils (SPEAC), and “equity-deserving” communities to ensure the unique needs of all diverse student populations are met.
- Using the funds in as flexible, private and stigma free manner as possible.

Spending descriptors include:

- Spending on food security students and families in addition to any planned or budgeted spending on food and meals programs.
- Spending that provides family assistance by way of offsetting costs for such things as school supplies, education related fees, clothing/footwear required for school sports and other school activities etc.

3

3



## Stakeholder Consultation



The Sooke School District is comprised of a diverse demographic and accordingly sought understanding of the needs of various groups including, but not limited to, Indigenous partners, parents/guardians and newcomer and refugee populations.

Per Ministry of Education and Child Care direction, the District engaged in consultation with Indigenous partners, the Sooke Parents Education Advisory Council (SPEAC) and other stakeholders to inform the development of this action plan. Consultations focused on developing an understanding of unique needs, prioritization of needs, barriers and stigma related concerns.

Input from stakeholders directly informed guiding principles and subsequent action steps set out in the District’s Student and Family Affordability Fund Action Plan.

4

4



## Guiding Principles



- Ensure that the funding is used in accordance with Ministry of Education and Child Care guidelines
- Creatively use the funds in as flexible, private and stigma free manner as possible
- Creatively use the funding to have as broad an impact as possible to ensure those most in need are supported
- Develop a multi-pronged approach that is a blend of school based, district based and community partnership-based initiatives
- Ensure ongoing consultation with stakeholders including, but not limited to, Indigenous Rights Holders, SPEAC and School PACs, Internal District Stakeholders and Community partner agencies
- Ensure the action plan is organic and flexible and can be adapted to meet changing needs and overcome unanticipated barriers that may emerge

5

5

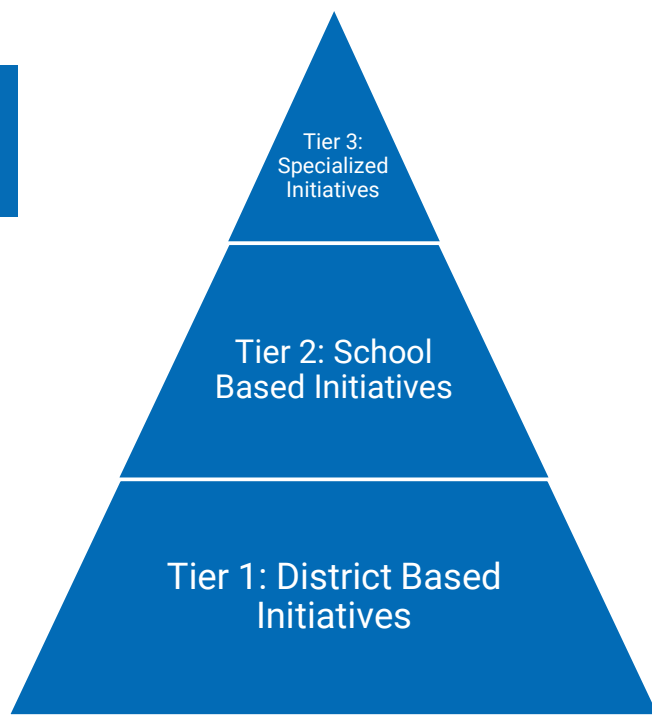


## Multi-Tiered Approach

**Tier 1 - District Based Initiatives:** These initiatives are organized and implemented at the district level in consultation with district stakeholders and include selected educational program fee relief at the elementary, middle, and secondary school level; expansion and development of existing and new school food programs; expansion and development of partnerships with third party community partners.

**Tier 2 – School Based Initiatives:** These initiatives are organized and implemented at the school level in consultation with local school stakeholders. Initiatives will focus on additional efforts to address food security, school supply costs, additional fee relief, access to clothing and equipment required for meaningful participation in school-based programs and activities.

**Tier 3 – Specialized Initiatives:** These initiatives are organized and implemented at the school and district level by specialized staff including our Safe and Healthy Schools team, in particular our team of School Based Social Workers. Initiatives will focus on additional efforts to address food security, school supply costs, additional fee relief, access to clothing and equipment required for meaningful participation in school-based programs and activities by those students and families most in need.



6

6



## Tier 1: District Based Initiatives



### Fee Relief: \$170,000+

The Affordability Fund is being used to offset universal education related fees at each school level.

**Secondary School Universal Fees:** The universal School Activity Fee will be waived for the 2022-23 school year. This fee is charged to offset costs related to student locks, lockers, school and classroom apps, and school activities and events.

**Middle School Fees:** The universal fees for ADST courses will be waived for the 2022-23 school year. These fees are charged to cover consumable materials used in each course area such as Textiles, Home Economics, Woodworking etc.

**Elementary School Fees:** Unlike middle and secondary schools, elementary do not publish fee schedules. However, throughout the course of the year costs may be incurred for educational field trips and events. Elementary schools will be provided funds in their school fund allocation to waive fees as broadly as possible in a stigma and barrier free manner.

7

7



## Tier 1: District Based Initiatives

### Food Security and Student Family Assistance: \$400,000

The Affordability Fund is being used to address food security and other affordability issues for students and families. This is being actioned through new and existing community partnerships in several ways. Examples include:

#### Sooke Food Bank

JMS breakfast program; Grab and Go snack program for all interested schools; holiday hampers; other essentials.

#### Sooke Family Resource Centre

Food, transportation and other life essentials provided via various services to local families.

#### Military FRC

Support "connection time" for families during deployment, providing a meal, childcare and social time.



#### Goldstream Food Bank

Hampers, emergency food and household supplies - available via 3rd parties like SBSW.

#### Salvation Army

Food fridge and social time at Langford based drop-in resource centre. Weekly grocery bag available. Monthly and Holiday hampers.

### Setting the Table: School Food Pilot Program



This partnership is a new food security pilot program aimed to delivery locally sourced prepared breakfast and lunches to schools. Committed partners include:

- SD62 school and district administrators
- SD62 culinary arts and food studies teachers
- Mustard Seed Food Security Distribution Centre
- Food Share Network
- Farm to School BC
- Victoria Community Food Hubs Society
- BC Chapter of the Coalition for Healthy School Food
- Island Health
- UVic School of Public Health and Social Policy

#### BGC South VI

Through Community Intervention Coordinators, provide food security and other essentials (e.g., transportation) to youth/families during out of school time.

#### Expansion of Current Programs

Includes, but not limited to, expansion of Truffles lunch program as well as expansion of Backpack Buddies program to all schools.

8

8



## Tier 2: School Based Initiatives



### **School Based Allocations: \$600,000**

The significant portion of the Student and Family Affordability Fund is being distributed to individual schools to action in a manner that best suits their school community. Each school community has its own unique context and school staff will be working with school Indigenous partners, Parent Advisory Councils, and community partners to create plans to meet student and family needs. Funds are to be used to address food security and other affordability issues for students and families.

Allocations will be based on several factors including school enrollment and other criterion. Schools will be expected to develop an action plan and have the expectation of expending funds by June 30<sup>th</sup>, 2022.

9

9



## Tier 3: Specialized Initiatives



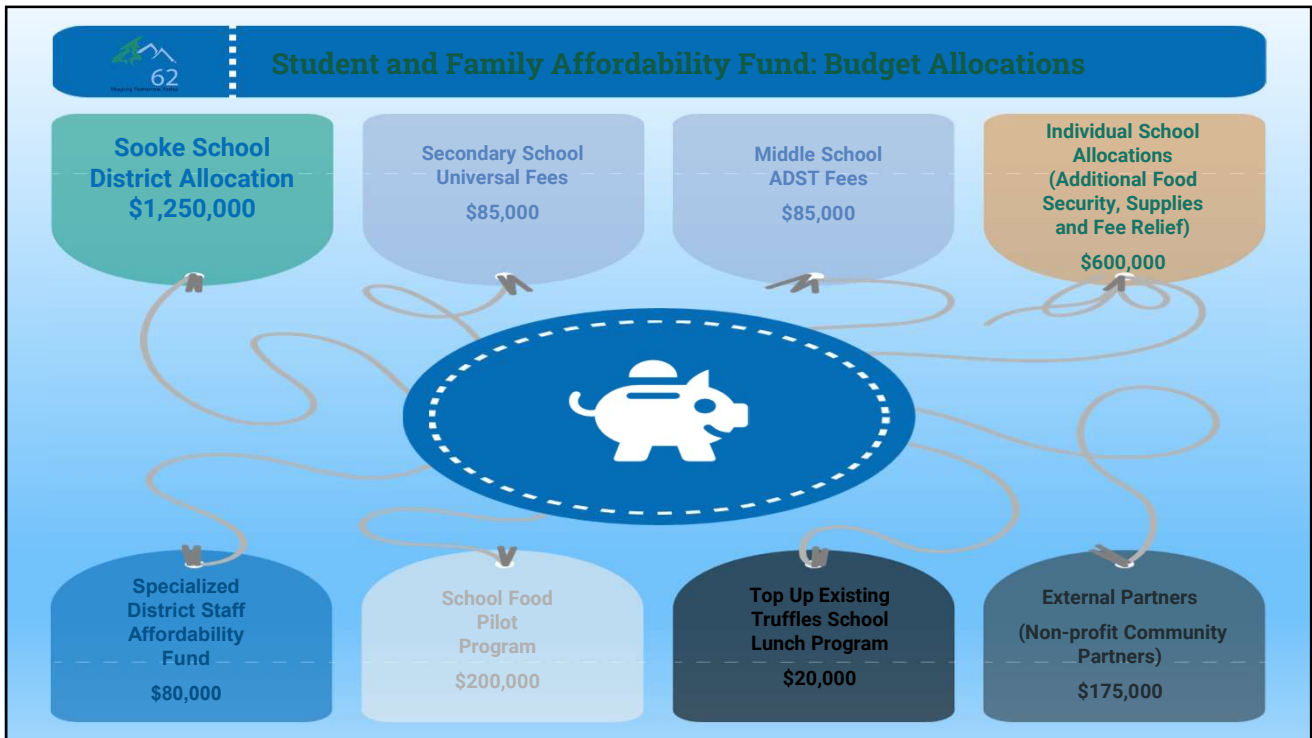
### **Specialized Initiatives: Emergent Response Fund: \$80,000**

The District has a dedicated group of professional that work directly with our most vulnerable students and families. These specialized staff will be provided an emergency fund to respond to significant hardships that unexpectedly emerge during the year and will provide them the resources to respond in a time sensitive and impactful manner.

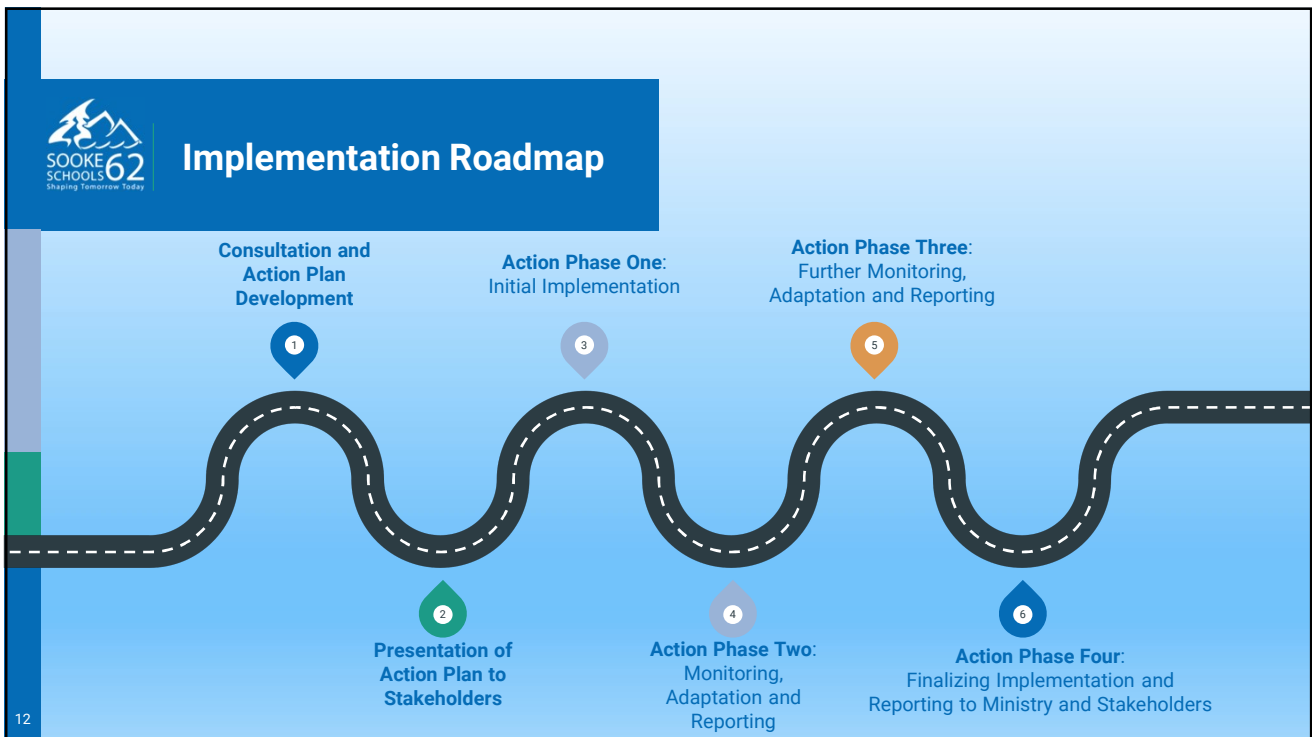
Initiatives will be organized and implemented at the school and district level by these specialized staff including, but not limited to, our Safe and Healthy Schools team, in particular our team of School Based Social Workers. Initiatives will focus on additional efforts to address food security, school supply costs, additional fee relief, access to clothing and equipment required for meaningful participation in school-based programs and activities by those students and families most in need.

10

10



11



12