



435 Hammonds Plains Road, Bedford, NS, Canada, B4B 1Y2  
☎ 902 835-8548 📠 902 835-9752 🌐 [sandylakeacademy.ca](https://sandylakeacademy.ca)

## Bring Your Own Device (BYOD) Policy

Sandy Lake Academy is dedicated to providing a learning environment that makes knowledge and information accessible and directs students to become more productive and responsible in their use of electronic devices. In line with provincial and federal laws, we have established this Bring Your Own Device (BYOD) policy to govern the use of personal electronic devices while on school premises. Through this policy we seek to ensure that student use of technology is safe, appropriate, and conducive to the Christian values and principles that we promote. This BYOD policy applies to all students during school hours and school-sponsored events on or off campus. This BYOD policy is in compliance with provincial and federal laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Education Act of Nova Scotia.

### 1. Objectives

The purpose of this BYOD policy is to establish guidelines for the responsible and secure use of personal electronic devices by students, ensuring compliance with relevant provincial and federal laws and regulations. Our objectives include:

- Ensuring all students have access to instruction and content that is engaging and student-centered where inquiry and authentic learning are emphasized.
- Focusing on learning, including critical and creative thinking, content evaluation, collaboration, self-direction, and personal responsibility in meeting specified academic goals.

### 2. Definition

BYOD refers to any personally-owned internet-enabled device used to complete assignments, projects, and other work. These devices include, but are not limited to: laptops, tablets, iPads, and chromebooks. Smartphones are not included under this policy.

### 3. References

- Discipline/Behavioural Policy (SLA Parent-Student handbook, p. 23-26)
- Harassment and Abuse Policy (SLA Parent-Student Handbook, p. 27)
- Technology Policy (SLA Parent-Student Handbook, p. 35)
- Personal Handheld Electronic Device Policy (Smartphones)  
<https://sandylakeacademy.ca/wp-content/uploads/2023/08/Electronic-Device-Policy-Update.pdf>

See **SLA Parent-Student Handbook** -

<https://sandylakeacademy.ca/wp-content/uploads/2023/08/2324-SLA-Parent-Student-Handbook.pdf>

### 4. Device Specification

Size or form factor laptops and tablets

- **Network connectivity:** Wi-Fi connectivity compatible with WPA2-Enterprise
- **Operating system and standard software:** Chrome OS, iOS, Mac Os and Windows
- **Security measures:** Student devices should not use Private Wi-fi Address. This might prevent connection to the network.
- **Battery runtime:** Devices should be in good working condition when it comes to battery.

## 5. Lightspeed Agent Content Filtering

Sandy Lake Academy uses two content filtering tools, provided by Meraki and Lightspeed Systems.

Meraki content filter is applied at the network level while Lightspeed Systems is applied at the device level.

Meraki Content Filtering is a robust web content filtering and security feature offered by Cisco Meraki, a leading networking and cloud management platform. This service is designed to help organizations, including businesses and educational institutions, maintain control over their network's internet access and ensure a secure and productive online environment. Meraki Content Filtering allows administrators to define and enforce web usage policies, block or allow specific websites or categories of content, and gain insights into network activity through real-time reporting and analytics.

Lightspeed Systems Filter is a comprehensive web content filtering and security solution designed to protect and manage internet access for educational institutions and other organizations. It employs advanced technology to monitor and restrict internet activity, ensuring a safe and productive online environment for students, staff, and users. The system filters websites, blocks inappropriate content, and provides granular control over web access policies. It also offers real-time reporting and analytics to help administrators monitor and analyze web usage, enabling them to make informed decisions about internet safety and compliance. Lightspeed Systems Filter is a valuable tool in maintaining a secure and controlled online ecosystem in educational settings.

## 6. Digital Classroom

In order to foster a productive and secure digital learning environment, SLA uses the Lightspeed Systems Classroom software that as features such as screen sharing, application control, web filtering, and communication tools. Lightspeed Systems Classroom is an innovative and versatile classroom management software designed to enhance the teaching and learning experience in a educational setting. This powerful tool empowers educators to effectively manage and monitor student devices in a digital classroom environment. With Lightspeed Systems Classroom, teachers can view, control, and interact with students' screens, ensuring that they stay on task and engaged in the learning process. Lightspeed Systems Classroom is a valuable resource for educators looking to harness the benefits of technology while maintaining a structured and effective classroom atmosphere.

## 7. Lightspeed Agent

Lightspeed Systems Agent is a crucial component of the Lightspeed Systems suite of educational technology solutions. This agent is a lightweight software application installed on student and staff devices, serving as a bridge between the users and the comprehensive web filtering and security features provided by Lightspeed Systems. The agent helps ensure that internet access and device usage are managed in accordance with the organization's policies, offering real-time monitoring and reporting capabilities to administrators. It allows for granular control over web content filtering, application usage, and device management. The Lightspeed Systems Agent plays a vital role in maintaining a secure and productive online environment for educational institutions, enabling them to strike the right balance between fostering technology-driven learning and ensuring a safe and

controlled digital ecosystem.

BYOD students devices are required to install the lightspeed agent on their devices and not remove it.

Sandy Lake Academy will monitor and filter network traffic on the school's Wi-Fi network to ensure the safety and security of students and to comply with provincial and federal laws, including the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

## 6. Actions

### Parents/Students

All students in grade 7-12 are invited to use a computing device at school each day. This device must be:

- An assigned device supplied by the school, or
- A personal device of student's own choosing and ownership which meets the **Device Specification (see #4)**.

### Responsibilities

1. The personal device must be able to be brought to school on each and every school day and be solely the student's to use throughout the school day.
2. Students and parents are responsible for ensuring the device brought to school meets all the requirements of the Device Specification. A device which does not meet the specification will not be permitted access to school networks and services.
3. Students requiring the use of an alternate device, for medical or therapeutic reasons, which does not meet the Device Specification must apply for and receive an exemption from the specification before bringing such a device. The application should state the reason for the request for exemption.
4. Prior to bringing a personal device for the first time, students and their parents must read and sign the **BYOD User Agreement** which sets out the responsibilities and expectations for use of the personal device at SLA.
5. Students must use their device in accordance with the aforementioned policies in the References section above.
6. Students must follow teachers' directions as to appropriate use of their devices in class.
7. Each student is absolutely and solely responsible for the care and conduct of his own personal device while at school or at other school activities
8. Students will be given individual credentials to access the network via a specific SSID network. must connect their device to the designated wireless data network supplied by SLA using their own, individual user account credentials only. (you will want to review this) Students must not connect to any other network, wired, wireless or cellular. Students must not bridge the SLA School designated network to any other network.
9. Users must not remove the remote management option for their device.
10. Students are expected to use the school's network for educational purposes only. Access to explicit, offensive, or inappropriate content is strictly prohibited.
11. Students must respect copyright laws and avoid the distribution of unauthorized copyrighted materials.

### Best Practices for Student Accounts

Devices used by students at school and home should have two separate local accounts, one for school work and another for personal use. This allows for supervision to be applied via the student school account while keeping a user's privacy in their personal account. It's advisable for parents to set up their personal monitoring tools on their child's personal account.

### Disciplinary Measures

Violation of this policy will result in disciplinary action in accordance with the school's code of conduct.

Repeated violations may result in the temporary or permanent loss of BYOD privileges. Students and parents/guardians should promptly report any incidents of misuse, bullying, or unauthorized access to school staff.

## Teachers

Teachers will encourage and facilitate the use of students' devices in their classes where they deem appropriate. Use of students' own devices in class is, however, at the sole discretion of the teacher. Teachers will follow standard discipline procedures in case a student fails to bring their device, in the same manner as if a student fails to bring any other required material to class.

## School

### Responsibilities

1. Maintain a **BYOD Policy** that ensures all students have access to the computing resources that are required for their coursework.
2. Ensure a copy of the **BYOD User Agreement** is signed by each student and their parents prior to allowing the student's device to be brought to school.
3. Publish a **Device Specification** that describes the requirements for devices brought to school pursuant to the BYOD program.
4. Provide a wireless network with filtered Internet connection to which students may connect their BYOD program device.
5. Provide support to assist students with first bringing their device to school and establishing network connectivity with the BYOD program device.

Should a student's device fail to meet a requirement of the **Device Specification**, the school will not facilitate the student's access to any network or school services. The school may direct a student to cease bringing a device to school which does not meet all the requirements of the Device Specification.

### Damage/Troubleshoot/Inspection

1. SLA will not be held responsible for any damage or data loss, including losses resulting from connecting devices to the school's wireless network or power outlets.
2. SLA staff will not configure, troubleshoot, or repair student devices. The school's IT department will provide technical support for device connectivity to the school's network. Students are responsible for their devices' maintenance and security.
3. School officials may read, examine, or inspect the contents of any personal device upon reasonable suspicion that the contents or recent utilization of the device contains evidence of a violation of these or other rules and policies, as well as any local, state, or federal laws.

## 7. Privacy and Confidentiality

1. Students must not take photos or make video or audio recordings of any individual or group without the express permission of each individual being recorded and the permission from a teacher.
2. Students must not publish material of any individual or group to the internet, including sites such as Youtube, Facebook Snapchat, Instagram, TikTok, etc. The school does not accept liability for material published.
3. Never publish or disclose the personal information of a staff member or students without the person's explicit permission. Personal information includes, but is not limited to, names, addresses, photographs, credit card details and telephone numbers of themselves or others.
4. Ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

## 8. BYOD User Agreement

The school administration may amend this policy as needed to adapt to changes in technology or legal requirements. By adhering to this BYOD policy, students and their families agree to comply with all its provisions

and acknowledge that the school has the right to monitor and access devices to ensure a safe and appropriate learning environment.

**Student Device Information**

**Brand:**

**Model:**

**Wi-Fi Mac Address:**

**Serial Number:**

**Agreement**

By signing below, you are agreeing that the student will abide by the BYOD policy, and that failure to do so will result in the consequences outlined in the policy.

**Student Name** \_\_\_\_\_

**Student Signature** \_\_\_\_\_

**Parent Signature** \_\_\_\_\_

**Date** \_\_\_\_\_