Bring Your Own Device (BYOD) IT Policy Student 2020

Dear students and parents,

1. Introduction

a. In the context of this policy, the term "device" refers to any mobile electronic technology, including assistive technologies, brought into The School, which is owned by the student, and which has the capability of connecting to The School's Wi-Fi network.
b. BYOD is an optional strategy. The decision to implement BYOD in schools remains with the School in consultation with its community.

2. Policy Requirements

a. Students are allowed to bring devices to School for the purpose of work and learning.
b. For the purposes of this policy, permitted devices include notebook computers (e.g. Windows, Mac OS, Android, Chrome OS) and tablet devices (e.g. Android, iOS). No other device may be connected to The School's network without prior consent from the Head of School.
c. Students and their parents/caregivers must complete and return a signed BYOD Student Agreement prior to participation in BYOD.

3. Access to the Wi-Fi network and resources

a. Internet access through the School's Wi-Fi network will be provided on site at no cost to students who are enrolled in Elonera Montessori School.
b. The School provides 802.11 b/g/n Wi-Fi on the 2.4 GHz band. It is the student's responsibility to ensure that the BYOD device is supported for these standards.
c. No network resources other than internet connectivity will be available to BYOD devices.

4. Acceptable Use of Devices

a. The Head of School will retain the right to determine what is, and is not, appropriate use of devices at the School within the bounds of the Elonera Montessori School's policies, and NSW privacy and other legislation.
b. Students must comply with The School's policies concerning the use of devices at School while connected to The School's Wi-Fi network.
c. Students should not attach any School-owned equipment to their mobile devices without the permission of the Head of School or an appropriate staff member.
d. Students must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by The School.
e. Where Students are aware of means by which they could compromise the School's network as in (d) above, they must notify an appropriate Staff member immediately.
f. Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.
g. Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/caregiver consent for minors), and the permission of an appropriate staff member.
h. Students must not use The School's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature. Such use may result in disciplinary and/or legal action.
i. Where the School has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the Head of School may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, School disciplinary action may be appropriate or further action may be taken.
j. The consequences of any breaches of The School's BYOD policy will be determined by the Head of School in accordance with relevant Elonera Montessori School policies and procedures and accepted school practice.

5. Long-term care and support of devices

a. Students are responsible for ensuring the operating system, and all other software on their device, is legally and appropriately licensed.
b. Students are responsible for ensuring that any device listed at (10) below has a supported operating system, and that all services packs, updates and/or patches for such device hardware, operating system and software, are applied per The Schools Charter of Respect and Responsible Use of Technology policy.
c. Subject to this agreement, and where appropriate, The School will install its recommended antivirus/antimalware solution (Webroot Secure Anywhere). This software will automatically update when the computer is connected to the internet. The student and their parents/caregivers indemnify Elonera Montessori School for any costs associated with the function and/or malfunction of this software.
d. Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. The School is not responsible for providing BYOD charging facilities.
e. Students are responsible for securing and protecting their device at School, and while travelling to and from School. This includes protective/carry cases and

exercising common sense when storing the device. The School is not required to provide designated or secure storage locations.

f. Students should clearly label their device for identification purposes. Labels should not be easily removable.
g. Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

6. Damage and loss

a. Students bring their devices onto The School site at their own risk.
b. In cases of malicious damage or theft of another device, existing School processes for damage to School or another student's property apply.

7. Insurance

a. Student devices are not covered by The School's insurance in the case of loss or damage. Insurance is the responsibility of parents/caregivers and students.

8. Technical support

a. The School provides no technical hardware or software support for any device listed at (10) below.

9. Security and device management processes

a. All devices connected to the Elonera Montessori School Wi-Fi Network are connected using a dedicated username and password for each user. Sharing of this information may result in the disabling of the account or removal of the BYOD device from the network.
b. Each BYOD device has a unique identifier referred to as a MAC address. BYOD access to The School's Wi-Fi network will be limited to MAC address listed below.
c. No device monitoring or remote access software will be installed on BYOD devices.
d. The status of The School's antivirus/antimalware software will be reviewed on a regular basis. Students whose device has a virus, or has out-of-date antivirus, may be contacted to resolve the issue.
e. Students who attempt to use a BYOD device without following these requirements will not be given access passwords and will not be able to connect to The School's Wi-Fi network through their BYOD device.

10. Agreement

We accept the BYOD IT Policy terms outlined above and agree to adhere to these. *This agreement is valid until the end of the current school year.*

Student Name:	_____
Student Signature:	_____
Parent Name:	_____
Parent Signature:	_____
Date:	_____

OFFICE USE ONLY

DEVICE NAME:	_____
DEVICE MODEL:	_____
DEVICE SERIAL NUMBER:	_____
WI-FI MAC ADDRESS:	: : : : :