Bring Your Own Device (BYOD) Policy

This policy includes the definitions and guidelines related to procedures involved in the safe and responsible use of Personal Technology Devices at the school. It also outlines procedures for safe use of School Network and Wi-Fi and outlines the agreement between the school and students.

References to Hartland learners should be read as Pupils in the Primary phase and Students in the Secondary phase of the school and are interchangeable.

Updated September 2024

Introduction

The UAE Vision 2021 clearly challenges us to address a *"complete transformation of the current education system and teaching methods. The National Agenda aims for all schools, universities and students to be equipped with Smart systems and devices as a basis for all teaching methods, projects and research".*

We already use a variety of technology, software and tools to support outstanding opportunities and engagement in learning. However, in order to maximise opportunities for students and teachers to use technology effectively and efficiently, the school will implement a Bring Your Own Device (BYOD) policy which asks students to bring a personally owned device to school to support and enhance learning, with effect from September 2020. Having constant access to a device will allow classrooms to increase learning opportunities and support collaboration through technology.

This policy pertains to students in Year 5 upwards and it sets out the usage agreement and responsibility of students to use devices and the internet safely in school.

This policy also includes two appendices:

Appendix 1 AI Guidance Document
Appendix 2 Acceptable User Agreement

Definitions

For the duration of this policy and its application to Hartland international School, Personal Technology Devices, School Use and School Network will be defined as below:

- A Personal Technology Device (PTD) is any form of mobile device. For the purpose of this
- policy, PTD's are limited to Laptop Computers and Surface Pro or Chromebook tablets only.

- School Use is limited to lessons and or enrichment activities, supervised by Hartland International School staff and in the case of older students, independent study, research and coursework completion during study time.

- The School Network includes any files or storage areas covered by the Office 365 suite registered to a school email address and any connection of PTD to the school password protected Wi-Fi.

We believe that it is essential that students have a laptop rather than a tablet or iPad.

The only exception to the tablet rule is the Microsoft Surface Pro or the Google Chromebook.

As we found from our DLE experience, a laptop is far more versatile as a tool for creation and completion of work. While other mobile devices like iPads and phones are great for researching, planning, and collaborating, they have their limitations when creating documents and we do not consider them a suitable BYOD device. Whilst we also accept that mobile phones are very much part of our culture and day-to-day life, this policy reinforces the fact that students are not allowed to use their mobile phones during the school day unless expressly instructed to or given permission to do so by a teacher.

Statement

All students in Year 5 to Year 11 are required to bring a PTD to school to support their learning. Hartland International School expects all students to be responsible digital citizens. Failure to adhere to the BYOD policy as detailed below will result in a denial of access or further sanctions as deemed appropriate by the Principal.

In addition to these year groups, some Students of Determination in other years may bring laptops as per their case by case recommendation of the Educational Psychologist.

Device Specifications

The computing environment in Hartland is PC based. This means that our network and printing options are designed around this. In order to optimise this environment, in terms of brands, we recommend a PC (windows) based laptop, Surface Pro or a Chromebook. If you are considering purchasing a new machine, do consider its weight as well as the basic requirements as students will carry this daily to and from school.

However, if you already have a MacBook Pro or a MacBook Air, please do not go out and buy anything new: just be aware that we are unable to offer technical support for Apple products at school and there can be some challenges with connectivity to school applications.

Device Specifications dictate the minimum acceptable functionality of a device for it to be suitable for use as part of the BYOD policy. All PTD should meet the requirements as listed below to be deemed suitable as part of the BYOD policy.

Each PTD must comply with the following:

- Dimensions: 10" screen size or larger
- Processor: Intel Core ™ i5 or better
- Memory: At least 4GB but 8GB preferred
- Operating System: Windows 10 or Mac OS 10.15.5
- Hard Drive: 128 - 256GB SSD*
- Wi-Fi capable (802.11a/b/g/n/ac)
- Have capability to run Office 365 (online and downloaded applications)
- Up-to-date Anti-virus software (AVG free is recommended based on performance and cost reasons)
- 2 or more USB 2.0 / 3.0 slots.
- Have a physical keyboard (attached or inbuilt)
- 6 + hour battery life.
- Be password operated by the student
- Robust headphones or earbuds should be brought also

The school will not be able to provide replacement or spare headphones and as such 'high build quality products' should be purchased if possible so as to ensure longevity of life.

Please also note that students should avoid using their PTD to store personal music and video as it will quickly use up storage which will affect system performance.

Protection

It is highly recommended that all PTDs should have the necessary protection to prevent any accidental damage that could occur to the screen, device or any other components. It Is recommended that you purchase:

- A suitable protective case or cover for transport to and from school
- For Surface Pro's or Chromebooks, a hard case that protects the screen
- Suitable insurance or a warranty that covers school and home usage

Device covers, desktop backgrounds and screensavers should be as per the make and model brand or plain in colour. Alternatively, any decoration or design should be appropriate for school use.

Security, theft or damage

- BYOD devices and/or any peripheral hardware are the sole responsibility of the student.
- Hartland International School accepts no responsibility for the security or safety of the device or any peripheral hardware, and as per protection guidance, suitable insurance should be secured.
- Students are responsible for the security of their device and any peripheral hardware. If placed into the provided locker, lockers should be locked at all times in secondary phase. Classrooms will be locked and secured during playtime in the primary phase.
- Teachers and other staff will not store or hold onto devices or any peripheral hardware.
- IT staff and technicians will support and troubleshoot student devices or any peripheral hardware for everyday issues, but they will not repair or troubleshot beyond the most basic of normal support.
- Theft or vandalism of any kind should be reported immediately to a school administrator.

Monitoring and Device Management

To promote a safe digital environment, the school employs the following measures:

- All school iPADS are monitored using Mosyle which limits functionality and restricts access to content.
- All students in Years 5-13 are required to bring their own device to school and must sign the Hartland Acceptable Use Agreement prior to receiving their login details.
- All parents of students receive a copy of the Bring Your Own Device (BYOD) Policy which clearly outlines school procedures and is available on the school website.
- Student Wi-Fi Network access is limited to a single source which is controlled by Fortinet, a firewall system that restricts internet access and is controlled by the school.
- The Meraki firewall system logs staff and student connections to different access points in the school.
- Each student has a unique username and password to the school Wi-Fi, at any point their internet access, search history and browser history can be accessed.
- Students must hand in mobile phones at the beginning of each school day in Years 6-11 to ensure that restricted websites, applications or content cannot be access through use of mobile data.

User Guidelines

- Devices should be fully charged at the beginning of the day.
- Devices should be able to run independently, without connection to a power source.
- If damaged, lost, stolen or unable to function, devices will be repaired or replaced in a timely manner.
- Devices should never be shared or lent to other students from Hartland International School or other schools.
- Access to the School Network is restricted to members of the Hartland International School community and should not be shared with others.
- A charging device will be brought to school every day to ensure that the device can be used throughout the school day.

Who was consulted?

In drafting this policy, Hartland International School has followed best practice globally and drawn on the expertise and experience of staff and Leadership at the school.

https://nationalcollege.com/courses/certificate-preventing-responding-to-cyberbullying#:~:text=Developed%20by%20Dr%20Claire%20Sutherland,respond%20to%20incidents%20of%20cyberbullying

Date for next review of policy

September 2025

Signed.....Date.....

School Principal

Relationship to other policies, guidelines and statements

- Behaviour for Learning Policy
- Child Protection Policy
- Anti-bullying Policy

Appendix 1

Hartland International School – AI Guidance Document

Artificial Intelligence
Artificial intelligence (AI) has become part of everyday life. As with any emerging or developing form of technology, it is important to learn how to use and interact with it safely as well as how to leverage its benefits.

Generative Artificial Intelligence
Generative AI is an algorithm that can be used to create new content, including but not limited to text, code, images or music.

Using generative AI to create work and present it as your own is wrong. This may take the form of submitting work not created by a student as part of an assessment to achieve a desired grade or, to produce content attempting to falsely demonstrate achievement or competence in a subject area. Generative AI or any other computer software should never be used with the intention to deceive others. This could be within school, at home or on social media platforms.

Student Code of Conduct
When using generative AI as part of your education, think about the following:

- If you are unsure, ask your teacher if generative AI can be used as part of the task or assignment.
- Be transparent about your use of generative AI and be prepared to explain how or why you used it to complete a task. This should also include giving credit or referencing sources you have used within your work.
- When you use generative AI, take time to read through the responses and consider what has been produced.
- Think carefully about the purpose of the task you have been given. Is it to develop skills by methodically working through a process using original thought or to critically examine something to gauge understanding?
- Consider potential bias in generated information as you would do with any other source.
- Think carefully about the kind of information you input into a platform, stop and consider the following questions:

1. Is this information personal?
2. Is this something I should share with other people?
3. Is this platform secure?
4. What is the motive to use this platform?
5. Who owns the platform and what is their motive for developing it?

Misuse
Where students fail to adhere to the code of conduct or knowingly submit work produced by AI against explicit instructions, appropriate sanctions will be issued depending on the severity of the situation and intent.

Digital Citizenship and Artificial Intelligence
Digital citizenship refers to the responsible and safe use of technology, including computers, the internet, and digital devices, to engage with society on any level. A digital citizen is anyone who regularly uses information technology and has both rights and responsibilities in relation to their actions online. The concept of digital citizenship involves not only laws and documentation but also the idea of belonging to a digital community. It includes protecting private information online, mitigating risks associated with cyber threats or online threats, and utilizing information and media in a knowledgeable and legal way. Good digital citizenship means behaving in a positive and helpful way online.

Many platforms use AI to curate content for you to interact with. Algorithms learn about your preferences, browsing habits and interests with the goal of making their platform more engaging. While there are benefits to this, there are also people who use software to gain information about you with the intention of doing harm.

Consider the following when spending time online:

- When I enter information into a platform, what can it be used for?
- Is the information I am giving mine, or does it belong to someone else?
- Could someone find out things I am uncomfortable with when I hand over this information?
- When I share an image of myself or any other personal content, can it be undone?
- If sharing or uploading an image of someone else, do I have their permission?
- If this content or information was accessed by someone else, what would the consequences be?

Positive Use of Artificial Intelligence

Although there are dangers and risks, there are many positive benefits that you can illicit by interacting with AI platforms. Positive uses of these could include:

- Creating revision guides or prompts to aid study.
- Checking the quality and accuracy of work and gaining ideas on how you can improve it.
- Solving problems you are stuck on and using AI to explain the steps behind solving the problem.
- Creating or generating ideas you might not have been otherwise able to come up with.
- Summarising notes and key concepts before and after lessons.
- Using AI tools to organise notes, resources and increase productivity.
- Leveraging your own skills to develop your own usage and understanding of different platforms for use in and out with school.
- Collaborating with others in the development of notes and resources.

Your Teachers Will:

- Give clear parameters to you about how and when you can use AI within your work.
- Provide you with opportunities to explore and learn how to use AI effectively.
- Create opportunities for positive dialogue and constructive criticism about your work and interactions with AI.
- Create learning opportunities for you to discuss the ethics behind AI development and how it will impact you.
- Challenge you if they think that you have submitted work that is not your own by drawing comparisons to work submitted or completed under exam conditions or completed without the aid of technology.
- Actively participate in discussions about the ethical use of AI and how it can be leveraged to improve educational experiences for students.

Review

This document will be reviewed annually in conjunction with teachers and students. However, should significant advancements in availability or capability of AI occur, this may take place at any time. Notice of any changes will be highlighted and shared with all relevant stakeholders.

Appendix 2

Acceptable Use Agreement

Use of a PTD whilst accessing the School Network in or out of school is in accordance with and agreement with the Acceptable Use Agreement below. All students and a parent or guardian are required to co- sign this agreement before access is granted.

1. Before use of your PTD is permitted, this agreement must be signed and returned by the student and a parent or guardian.
2. PTD are to be used only for School Use purposes in classrooms and learning areas under the guidance of teachers. Devices are not to be used for student-to-student general communication other than shared work groups.
3. Students should only access their specific WI-FI Network. They are not permitted to access Guest or Staff Networks.
4. No attempts should be made to navigate around, or access websites blocked by the school firewall. Including but not limited to VPN use, restricted applications or attempts to view material deemed against the Internet and Cybersecurity laws of the UAE.
5. Social Network access is not permitted unless it forms part of a lesson, directed and guided by a teacher.
6. Students may not capture or record any kind of pictures or videos of other students, members of staff, school employees or guests without first gaining their permission.
7. If there is reasonable suspicion that a PTD has been used inappropriately, staff have the right to ask to view the content of a PTD, including use history and downloaded or uploaded files.
8. No student shall establish a wireless ad-hoc or peer-to-peer network using their PTD or any other device in the school, including but not limited to 'Hot Spot' boosting from personal mobile devices.
9. Teachers may request, at any time, that PTDs are turned off in or out of the classroom and not accessed. Failure to follow teacher instructions may result in restriction of School Network access and denial of School Use.
10. Sound should be muted on all devices, unless requested to be turned on by teachers. Use of headphones may be required and permitted in some lessons.
11. Students should not attempt to log-in with the password of any other student or staff member.
12. All student passwords and log-in information are private and should not be shared with any other student.
13. Students are always personally responsible for their PTD unless given permission by a teacher for it to be stored in a lockable location.
14. Hartland International School can provide access support but not will provide repair or diagnostic services to PTDs.
15. In the future, the school may decide to install access limiting software on PTDs that restrict their use in the school network, including website access governance and limiting use of certain apps deemed not educational or part of School Use.
16. Each student is entirely responsible for their own PTD. The device should be treated responsibly and used with care. Hartland International School will accept no responsibility for PTDs that are damaged, lost, stolen, or which have data infected/corrupted. Teachers will help students identify how to keep personal technology devices secure, but students have the final responsibility for securing their devices.
17. The school will ensure that all students have appropriate training in relation to digital citizenship and staying safe online.

Personal Technology Device Acceptable Use Agreement	
Parent Name:	Signature:
Student Name:	Signature:
Class / Tutor Group:	
Date:	
Device Details: (optional to provide) Insurance/Warranty Details: (optional to provide)	