EMU HEIGHTS PUBLIC SCHOOL
Student Bring Your Own Device (BYOD) Policy
November 2017

This policy provides direction to schools choosing to allow student use of personal mobile electronic devices at school to access the Department of Education and Communities' wireless network.

1 Objectives – Policy Statement

- 1.1 The term "device" in this policy refers to any personal mobile electronic device with the capability to connect to the department's Wi-Fi network.
- 1.2 Schools can allow students to bring their own devices to school and may provide access to the department's Wi-Fi network.
- 1.3 Use of devices at school will be governed by school developed guidelines and processes based on the Bring Your Own Device Implementation Guidelines.
- 1.4 The department will provide internet access through its wireless networks at no cost to students enrolled in NSW Public Schools at DEC sites.
- 1.5 Students are responsible for the care and maintenance of their devices including data protection and battery charging.
- 1.6 The department will not accept any liability for the theft, damage or loss of any student's device. Students who bring their own devices onto school sites do so at their own risk.
- 1.7 Schools are not obliged to provide hardware or technical support for devices.
- 1.8 Students and their parents/carers must complete and return a signed BYOD Agreement prior to connecting to the department's Wi-Fi network.
- 1.9 Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Agreement, they may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, further action may be taken including referral to the police. School disciplinary action may also be appropriate.

2 Audience and applicability

- 2.1 This policy applies to students connecting a device to the department's Wi-Fi network.

3 Context

- 3.1 The increasing availability of personal technology has accelerated the demand for new models of learning, whereby students may be encouraged to bring their own devices to school.
- 3.2 Choosing to implement BYOD access can provide a process to allow schools and the department to efficiently incorporate student-owned devices into our digital learning environments while protecting school and DEC infrastructure and data.
- 3.3 This policy should be read and interpreted in conjunction with:
  - Code of Conduct Policy
  - Values in NSW Public Schools
  - DEC Privacy Code of Practice
  - Online Communication Services – Acceptable Usage for school students
  - Legal Issues Bulletin No. 35 November 2012 – Use of mobile phones, portable computer games, recording devices and cameras in schools
  - Legal Issues Bulletin No. 8 September 2012 – Claims for loss of or damage to personal property
  - Smartcopying – Copyright guide for schools.
- **3.4 Document history and details (to be left in bold)**
  - Policy title
  - Student Bring Your Own Device Policy (BYOD)
  - Implementation date

- 2013-11-26
- Web publication date
- 04/07/2014
- Reference Number
- PD/2013/0458/V01
- Approval date
- 2013-11-11
- Approving officer
- Chief Information Officer, Information Technology Directorate
- Superseded documents

4 Responsibilities and Delegations

- 4.1 *Principals* are responsible for the implementation of this policy and guidelines in their school and are required to ensure that this policy is followed by participating *students* and their *parents/carers*.
- 4.2 *Principals* are responsible for dealing with any breach of the BYOD Agreement as outlined in the Bring Your Own Device Implementation Guidelines.
- 4.3 *The department* conducts surveillance and monitoring of its computer systems to ensure the ongoing confidentiality, integrity and availability of services.

5 Monitoring, evaluation and reporting requirements

- 5.1 Principals will supervise the implementation of the policy and report their evaluations to their Director, Public Schools NSW.
- 5.2 ITD will update this policy and the guidelines referenced as technologies change or as required.

STUDENT BRING YOUR OWN DEVICE (BYOD) DEC GUIDELINES

1. Policy requirements

1.1 Schools can allow students to bring devices to school for the purpose of learning.

1.2 Use of devices at school will be governed by school-developed policies that involve community consultation.

1.3 Prior to implementing BYOD, schools should provide information to key community stakeholders including teachers, parents, caregivers and students.

1.4 Students and their parents/caregivers must complete and return a signed BYOD Student Agreement prior to participation in BYOD.

1.5 The school and its community can choose the BYOD model that is relevant and appropriate for the needs of the students and the community.

1.6 Prior to implementing BYOD, schools should consider/identify strategies to ensure that all students are able to engage fully in classroom activities. This should include strategies to accommodate students without a device.

2. Access to the department's Wi-Fi network and resources

2.1 Internet access through the department's Wi-Fi network will be provided on departmental sites at no cost to students who are enrolled in NSW public schools.

2.2 Access to school resources such as shared drives, printers and associated costs will be a school-based decision.

3. Acceptable use of devices

The principal will retain the right to determine what is, and is not, appropriate use of devices at the school within the bounds of the department's policies and NSW privacy and other legislation.

Schools should review existing policies and processes to include the BYOD policy, where appropriate.

3.1 Students must comply with departmental and school policies concerning the use of devices at school while connected to the department's Wi-Fi network.

3.2 Mobile phone voice and text, SMS messaging or device instant messaging use by students during school hours is not permitted and doesn't form part of this policy..

3.3 Students should not attach any school-owned equipment to their mobile devices without the permission of the school principal or an appropriate staff member.

3.4 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 department, its Information Technology Directorate or the school.

3.5 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

3.6 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) being recorded and the permission of an appropriate staff member.

3.7 Students must not use the department's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in disciplinary and/or legal action.

3.8 Students and their parents/caregivers are advised that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the principal 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 including referral to the police.

The consequences of any breaches of the school's BYOD policy will be determined by the principal in accordance with relevant Department policies and procedures and accepted school practice.

4. BYOD Student Agreement

Schools must ensure that students and their parents/caregivers are aware of, and agree to their obligations under the school's BYOD policy and other relevant departmental policies.

4.1 Prior to connecting their devices to the department's Wi-Fi network, students must return a BYOD Student Agreement.

4.2 The BYOD Student Agreement contains both BYOD Device Requirements and BYOD Student Responsibilities.

4.3 The BYOD Student Agreement must be signed by the student and by a parent/caregiver. If a student is living independently of their parents/caregivers or is 18 years of age or more, there is no requirement to obtain the signature of a parent/caregiver. Principals will make these determinations.

4.4 By accepting the terms of the BYOD Student Agreement, the student and parents/caregivers acknowledge that the student:

- agrees to comply with the conditions of the school's BYOD policy; and

- ❖ understands that noncompliance may result in disciplinary action.

Schools should retain a copy of the BYOD Student Agreement in print or electronic form and it should be kept on file with the student record.

5. Long-term care and support of devices

Students and their parents/caregivers are solely responsible for the care and maintenance of their devices.

5.1 Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the BYOD Student Responsibilities document.

5.2 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

5.3 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. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.

5.4 Students are responsible for securing and protecting their device in schools, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.

5.5 Students should clearly label their device for identification purposes. Labels should not be easily removable.

5.6 Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

6. Damage and loss

6.1 Students bring their devices onto the school site at their own risk.

6.2 In cases of malicious damage or theft of another student's device, existing school processes for damage to school or another student's property apply.

7. Technical support

Schools are under no obligation to provide technical support for hardware or software. Schools may choose to provide this service to students if there are sufficient resources available in the school.

- ❖ Online Communication Services – Acceptable Usage for School Students.

8. Insurance

Student devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents/caregivers and students.

9. DEC technology standards

Schools should be aware of the following essential information regarding technology standards for devices used within schools.

9.1 The department's Wi-Fi network installed in high schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect.

9.2 The department's Wi-Fi network installed in most primary schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect. There

may be some variation to this standard in some primary schools. The IT delegate in the school will be able to provide details.

10. Device requirements

The BYOD Device Requirements' document and the BYOD Student Responsibilities' document should be developed to suit the school's purpose and should contain recommendations relating to:

- Departmental technology standards
- Hardware specifications, including the operating system
- Software and apps
- Battery life/spare batteries/battery charging
- Protective casing (scratch/impact/liquid-splash resistant)
- Device insurance/safety
- Ergonomics
- Back-up storage such as portable hard drive or USB flash drive.

11. Security and device management processes

Depending on the model of BYOD a school chooses, the following considerations are essential:

- strong passwords (the portal has Password Help information);
- device anti-virus software, if applicable; and
- privacy controls.

The department's Digital Citizenship (www.digitalcitizenship.nsw.edu.au) website contains information to support security and device management.

12. Suggested process for community consultation and school policy development

Schools in consultation with their communities should determine whether the school will implement BYOD. Teaching and learning should be the key driving force for this decision.

The following is a suggested approach to the decision-making process.

CONSULTATION	Action	Resources
Step 1	Provide information to the school community including staff, students and parents/caregivers	Staff discussion Information to students and parents/caregivers Literature review
Step 2	Survey attitudes Develop own survey instrument or use all or part of existing survey tools Interpret the data	Survey to key stakeholders- staff, students, parents/caregivers

Step 3	Hold a school staff meeting, P&C meeting, parent/caregiver/student forum after the surveys have been analysed	Present findings Clarify the next steps, if BYOD is going ahead
POLICY DEVELOPMENT		
Step 4	Form a BYOD interest group	Representation from executive, staff. parents/caregivers (P&C) and, if appropriate, students (SRC for example)
Step 5	Develop a draft BYOD policy for the school, including strategies to address any equity considerations	DEC's policy document and implementation guidelines Draft school policy document
Step 6	Circulate the draft school policy for comment by the school community	Feedback form
Step 7	Develop the final version of the policy	BYOD interest group Advice from feedback form
Step 8	Communicate the school's BYOD policy to the school community	BYOD policy document and accompanying letter
Step 9	Plan a review/evaluation cycle	

13. Suggested structure for a school BYOD policy

Rationale

Why is this policy being written? What does the school and its community believe about the educational value of using students' personal mobile devices in the classroom?

This section might also contain background information about the school and its values and any other relevant factors relating to the policy.

Policy statement

A brief statement about **what** the policy hopes to achieve.

Implementation

This section describes what BYOD means in the context of the school and **how** the policy will achieve its aims. Responsibilities and requirements of schools, staff, students and parents/caregivers are included and clear information regarding breaches of the BYOD policy is provided.

The BYOD Student Agreement along with the BYOD Student Responsibilities' document and the BYOD Device Requirements' document are located in this section.

Monitoring, evaluation and review

Outline when and how the policy will be monitored, evaluated and reviewed.

STUDENT BRING YOUR OWN DEVICE (BYOD) POLICY DEC GUIDELINES

1. Introduction

- This document provides advice and direction to schools choosing to allow student use of personal mobile electronic devices at school to access the Department of Education and Communities' wireless network.

- 1.1 The term "device" in this policy refers to any personal mobile electronic device with the capability to connect to the department's Wi-Fi network.

- 1.2 Schools can allow students to bring their own devices to school and may provide access to the department's Wi-Fi network.

- 1.3 Use of devices at school will be governed by school developed guidelines and processes based on the Bring Your Own Device Implementation Guidelines and the needs of the school.

- 1.4 The department will provide internet access through its wireless networks at no cost to students enrolled in NSW Public Schools at DEC sites.

- 1.5 Students are responsible for the care and maintenance of their devices including data protection and battery charging.

- 1.6 The department will not accept any liability for the theft, damage or loss of any student's device. Students who bring their own devices onto school sites do so at their own risk.

- 1.7 Schools are not obliged to provide hardware or technical support for devices.

- 1.8 Students and their parents/carers must complete and return a signed BYOD Agreement prior to connecting to the department's network.

- 1.9 Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Agreement, they may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, further action may be taken including referral to the police. School disciplinary action may also be appropriate.

2. Student BYOD Agreement

- 2.1 Prior to connecting their devices to the network, students must return a Student BYOD Agreement. A sample is provided which schools are able to modify to suit their BYOD model. This agreement must be signed by the student and by a parent/carer. If a student is living independently of their parents or is 18 years of age or more, there is no requirement to obtain the signature of a parent.

- 2.2 It is important to ensure that students are aware of and agree to their obligations under the Student Bring Your Own Device (BYOD) Policy and relevant policies, prior to using their own device on the DEC Wi-Fi network. School staff should endeavour to ensure that the BYOD student responsibilities are clearly understood by both students and their parents or carers.

- 2.3 The Student BYOD Agreement is a simple document with the purpose of acknowledging acceptance and agreement of the terms associated with the school's implementation of the Student Bring Your Own Device (BYOD) Policy by both students and parents/carers. It is accompanied by an Information Sheet that must be provided in conjunction with the Student BYOD Agreement.

- 2.4 By accepting the terms, the student and parents/carers acknowledge that they:
  - agree to comply with the conditions of the Student BYOD Policy.
  - understand that noncompliance may result in the student being subject to school disciplinary action.

- 2.5 Student BYOD agreements should be retained in print or electronic form for future access as required.

3. Cost to Students

- 3.1 Internet access through the Department's network will be provided at no cost to students enrolled in NSW Public Schools at DEC sites.

- 3.2 Access to school resources such as shared drives, printers and associated costs will be a school based decision.

4. Student Responsibilities

- 4.1 Students are solely responsible for the care and maintenance of their BYO devices. This includes but is not limited to:
  - Managing battery life and regular charging of their device.
  - Labeling their device for identification purposes.
  - Purchasing and using device protective casing.
  - Ensuring the device is safe and secure during travel to and from school and throughout the school day.
  - Maintaining up-to-date anti-virus software and operating system on their device.
  - Taking insurance coverage of their own device to protect any accidental damage, theft or loss.

- 4.2 Students are responsible for managing the battery life of their device and acknowledge that the school is not responsible for charging their devices. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.

- 4.3 Students must have a supported operating system and current antivirus software installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions.

- 4.4 Students should not attach any school-owned equipment to their mobile devices without the permission of the school principal or their delegate.

- 4.5 Students should clearly label their BYOD device for identification purposes. Labels should not be easily removable.

- 4.6 Students are responsible for securing and protecting their device in schools. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.

- 4.7 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

5. Damage and loss

- 5.1 Students bring their devices onto the school site at their own risk. For advice on theft or damage of students personal devices refer to legal issue bulletins below:
  - https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin35.pdf
  - https://detwww.det.nsw.edu.au/media/downloads/directoratesaz/legalservices/ls/legalissuesbul/bulletin8.pdf

- 5.2 In cases of malicious damage or theft of another student's device, existing school processes for damage to schools or another student's property apply.

- 5.3 Schools should regularly review existing policies and processes to include BYO devices where appropriate e.g. Student Welfare and Fair Discipline Code.

Technical Support

- 5.4 NSW DEC staff are under no obligation to provide any technical support on either hardware or software.

6. Long-term care and support of BYODs

- 6.1 Students are solely responsible for repair and maintenance of their own device. It is not the school's responsibility.

- 6.2 Warranties: Students should understand the limitations of the manufacturer's warranty on their BYO devices, both in duration and in coverage. Under Australian consumer legislation, warranties usually last for one year, during which any manufacturing defects will be repaired or the device will be replaced (as per the specific terms and conditions of the manufacturer).

- 6.3 Extended Warranties: At the time of purchase, students may also purchase an optional extended warranty (past the standard warranty period) from the supplier/manufacturer of their device, during which any manufacturing defects that may occur will also be repaired.

7. Insurance

- 7.1 Student BYO devices are not covered by Treasury Managed Fund. When students purchase their BYO device, they may also purchase an optional insurance policy from the supplier of their device or a relevant insurance company. As mobile devices are subject to a higher risk of accidental damage, prior to signing up for an insurance policy, students should be fully aware of the details and limitations of the policy, including any excess charged for making a claim, and the name of the company that holds the policy. As a guide, a suitable BYOD device insurance policy should cover all types of BYOD devices and provide worldwide, replacement cost coverage against:
  - accidental damage,
  - damage from falls and liquids,
  - theft
  - fire
  - vandalism
  - natural disasters (such as floods, cyclones, earthquakes, tornados, water damage, and power surge due to lightning)

- **Acceptable use of BYO devices**
- 7.2 Using the DEC network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in legal and/or disciplinary action.

- 7.3 Students shall 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 Department, its Information Technology Directorate or the school.

- 7.4 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

- 7.5 Mobile phone voice and text, SMS messaging or device instant messaging use by students during the school hours is a school based decision.

- 7.6 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/carer consent for minors) being recorded and the permission of an appropriate staff member.

- 7.7 Students shall comply with departmental or school policies concerning the use of BYODs at school and while connected to the Department's network including:
  - Online Communication Services – Acceptable Usage for School Students.

- 7.8 The principal retains the right to determine what is, and is not, appropriate use of BYODs device at the school within the bounds of NSW privacy and other legislation.

- 7.9 The consequences of any breaches of this policy will be determined by the principal, in accordance with the school's welfare and discipline policies. As the student device is intended as a *personal learning tool* schools are encouraged to consider a variety of alternatives to ensure equitable access to continued learning opportunities.

8. DEC Technology Standards (This will need to be adjusted to reflect the BYOD model chosen by your school community, a sample is below using the "Bring your own whatever connects to the internet" model identified by Dixon and Tiernay in the literature review)

- 8.1 Prior to purchasing or using an already purchased device, parents and students should be made aware of the following technology standards required for devices used within schools:
  - The DEC wireless network installed in **primary schools** operates on the 802.11n **5Ghz** standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only will not be able to connect.
  - The DEC wireless network installed in **high schools** only operates on the 802.11n **5Ghz** standard. Devices with 802.11a/b/g or 802.11n 2.4Ghz only will not be able to connect.
  - The battery life of the device should be capable of lasting 5 hours minimum of constant use without charge.
  - Device hardware specifications must meet the minimum (ideally the recommended) specifications of the operating system and all applications.
  - Currently supported Operating System.

- 8.2 Other considerations when purchasing a device include:
  - Extended warranty
  - Device insurance
  - Protective casing (scratch/impact/liquid-splash resistant)
  - Additional or spare battery packs
  - Ergonomics (is this device comfortable to use for an entire school day)
  - Backup storage such as portable hard drive or USB flash drive

9. Security and device management processes

- Depending on the model of BYOD your school chooses, you will need to consider how the following will be implemented:
  - Strong passwords (your portal has Password Help information),
  - Device anti-virus software
  - Data and network traffic encryption
  - Privacy controls
  - Internet filtering
  - DEC technology infrastructure security
  - Student Cyber Safety

EMU HEIGHTS PUBLIC SCHOOL
BRING YOUR OWN DEVICE POLICY 2017

Emu Heights Public School is excited to introduce a 'Bring your own device' to our school in 2017. This means that the students in Stage 3 (years 5 & 6) can bring their own iPad to school every day to enhance and support their learning. **This is not a compulsory requirement.** Your child will not be disadvantaged if you chose to not send an iPad to school. We have a number of iPads and other technology that your child can access at times.

THE ADVANTAGES OF STUDENT OWNED DEVICES INCLUDE:

- Anytime, anywhere access to class resources, support and extension activities
- The ability to develop "digital" folders and exercise books for their activities
- Greater ability to communicate with teachers and peers to support their learning
- Access to unlimited resources and information on the internet
- The ability to draft, redraft and publish their work at the click of a button
- Allowing students to become independent, active partners in their learning
- Enhanced opportunities to learn by offering students virtual experiences and tools that save them time, allowing them to take their learning further.

BYOD GUIDELINES

- iPads are be covered under the EHPS Phone and Devices Policy
- The purpose of bringing the device to school is to support the student's learning.
- The school will not be held responsible for loss or damage to the device. Students bring their own device for use at Emu Heights Public School at their own risk.
- Emu Heights Public School does not warrant or support the device and may not be able to support any technical issues and/or upgrades of the equipment/device.
- The device is the responsibility of the student whilst at school just like any other piece of equipment they might bring to school.
- The device should be covered by the owner's insurance.
- Students will be responsible for their own device and will place it inside their classroom at the start of the day and leave it there. The device will return home and be charged at the end of each day.
- Security measures for safe storage will be provided from 855am, but ultimately the device is the responsibility of the student.
- Within school grounds students are not permitted to have their iPads turned on or out of their school bag unless directed by a staff member
- Students will only be able to use the device in-class under teacher supervision.
- The internet will only be accessed via the school Wi-Fi and through the student's portal logon (No 3G access)
- No software downloads or updates will be carried out at school on student owned devices The device is used at the class teacher's discretion and with the class teacher's knowledge.
- Photographing or videoing others is strictly prohibited
- Students must not let others use their device.
- If you are concerned that the device is going to be broken, lost or stolen, you may wish to opt out of allowing your child to bring their device to school.
- Standard school discipline procedures apply for misuse of the device contrary to the BYOD Agreement.

BYOD STUDENT RESPONSIBILITIES

Operating system and anti-virus:

Students must ensure they have a legal and licensed version of a supported operating system and of software. If applicable, students' devices must be equipped with anti-virus software.

NSW Department of Education and Communities' Wi-Fi network connection only:

Student devices are only permitted to connect to the department's Wi-Fi network while at school. There is no cost for this service.

Battery life and charging:

Students must ensure they bring their device to school fully charged for the entire school day. *No charging equipment will be supplied by the school.*

Theft and damage:

Students are responsible for securing and protecting their devices at school. *Any loss or damage to a device is not the responsibility of the school or the Department.*

Confiscation:

Students' devices may be confiscated if the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement.

Maintenance and support:

Students are solely responsible for the maintenance and upkeep of their devices.

Ergonomics:

Students should ensure they are comfortable using their device during the school day particularly in relation to screen size, sturdy keyboard etc.

Data back-up:

Students are responsible for backing-up their own data and should ensure this is done regularly.

Insurance/warranty:

Students and their parents/caregivers are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.

EMU HEIGHTS PUBLIC SCHOOL
BRING YOUR OWN DEVICE (BYOD) STUDENT AGREEMENT

Students who wish to take advantage of the BYOD policy must re must read and sign the BYOD Student Agreement in the company of a parent or caregiver unless otherwise directed by the principal. This page is to be signed and returned to the school. By signing this agreement, students agree to the following conditions and behaviours.

I agree that I will abide by the school's BYOD policy and the conditions outlined below:

- I will use the department's Wi-Fi network for learning and follow the Internet and email code of Practice that I have signed.
- I acknowledge that the school cannot be held responsible for any damage to, or theft of my device.
- I agree to store my device in the classroom storeroom during recess and lunch and when not being used at the direction of my teacher.
- I agree to be responsible for charging my device.
- I will use my device during school activities at the direction of the teacher.
- I will only work on tasks specified by my teacher.
- I will use my own portal/internet log-in details and will never share them with others.
- I understand that my activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.
- I will not use apps or go to websites that my teacher hasn't asked me to.
- I will stay safe by not giving my personal information to strangers.

- I will not use my own device to knowingly search for, link to, access or send anything that is:
  - offensive
  - inappropriate
  - threatening
  - abusive or
  - defamatory
  - considered to be bullying

.

- I will not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/carer consent for minors) being recorded and the permission of an appropriate staff member.
- I will not attach any school-owned equipment to my mobile device without the permission of the school.
- I will follow school guidelines and procedures when preparing material for publication, will abide by copyright and acknowledging the sources of my information.
- I will not hack or bypass any hardware and software security implemented by the department or my school.
- I will report inappropriate behaviour and inappropriate material to my teacher.
  I have read the BYOD Student Responsibilities document with my parents and agree to comply with the requirements.
- I have reviewed the BYOD Device Requirements document and have ensured my device meets the minimum outlined specifications.

I have read the NSW Department of Education and Communities' *Online Communication Services – Acceptable Usage for School Students. with my parents* and will abide by its contents.

Student Agreement

1. I have read and agree the terms and conditions for use of my personal device and technology resources at Emu Heights Public School.

2. I understand and will abide by the stated terms and conditions, using these resources in a responsible and respectful manner.

3. Should I commit any violation, I understand that my access privileges may be revoked, school disciplinary action may be taken and appropriate legal action could also result.

Student Name: ..... Year: ..... Roll Class: .....

Student Signature: ..... Date: .....

In the presence of

Parent/Carer Name: .....

Parent/Carer Signature: ..... Date: .....

Parent / Carer Agreement

- ❒ I agree to my child bringing and using his/her own device to school for educational purposes in accordance with the student agreement above.

- ❒ I understand that I am liable for all damage and problems that may occur to the device owned and /or supplied by me or my child.

- ❒ As the parent / caregiver of ……, I have read the terms and conditions for acceptable use of technology resources at Emu Heights Public School. I understand that the access to and use of digital technologies is designed for educational purposes only, and that the school and Department of Education and Training have taken precautions to eliminate controversial material.

- ❒ I understand that the school will provide adequate supervision and the steps have been taken to minimize risk of exposure to unsuitable material. and will not hold them responsible for unauthorised materials acquired on the network. I hereby give my permission for my child to access educational material on the network.

- ❒ I recognise that Emu Heights Public School and its system administrators will take all reasonable efforts to restrict access to controversial materials,

- ❒ I certify that the information contained in this form is correct

iPad Serial Number_____ iPad Colour_____

iPad model Number_____

Passcode/Password_____

___

Parent / Carer Signature:_____ Parent / Carer name: _____ Date: _____

BYOD DEVICE REQUIREMENTS

Wireless connectivity:

High schools: The department's Wi-Fi network installed in high schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect.

Primary schools: The department's Wi-Fi network installed in primary schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect.

Note: There may be some variation to this standard in primary schools. The IT delegate in the school will be able to provide details.

***Operating system*:**

The current or prior version of any operating system.

Software and apps:

School-based requirements. All software and apps should be fully updated.

***Battery life*:**

A minimum of 5hrs battery life to last the school day.

***Memory and RAM*:**

A minimum specification of 16 GB storage and 2 GB RAM *to process and store data effectively.*

***Hardware features*:**

Camera and microphone.

Ergonomics:

Reasonable sized screen and a sturdy keyboard *to enable continuous use throughout the day.*

Other considerations

Casing: Tough and sturdy to avoid breakage.

Weight: Lightweight for ease of carrying.

Durability: Durable and strong.

Accessories

Carry case: Supply a carry case or skin to protect the device.

Insurance and warranty: Be aware of the terms of insurance policies/warranties for the device. The school will not accept responsibility for loss or breakage.

Back-up storage: Consider a portable hard drive as an appropriate source of back-up storage for essential documents.

STUDENT AGREEMENT APPENDIX
DETAILED INFORMATION FOR PARENTS

Online Communication Services:
Acceptable Usage for School Students

Students will:

- ensure that communication through internet and online communication services is related primarily to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal e-learning account.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
  - a message that was sent to them in confidence.
  - a computer virus or attachment that is capable of damaging recipients' computers.
  - chain letters and hoax emails.
  - spam, e.g. unsolicited advertising material.
- never send or publish:
  - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  - sexually explicit or sexually suggestive material or correspondence.
  - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services is primarily used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.
-

Responsibility for device

Students should be aware that:

- the school accepts no responsibility for the theft, damage or loss of any device a student brings onto the school site
- hey bring their devices onto the school site at their own risk

Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

Intellectual Property and Copyright

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.

- ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

Misuse and Breaches of Acceptable Usage

- Students will be aware that:
- they are held responsible for their actions while using internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.
- If they are found with any inappropriate material on their device in breach of the agreement, the device may be confiscated and the matter reported to the police.

Monitoring, evaluation and reporting requirements

Students will report:

- any internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Communities.

Students should be aware that:

- their emails are archived and their web browsing is logged. The records are kept for two years.
- the email archive and web browsing logs are considered official documents.
- they need to be careful about putting their personal or sensitive information in emails or on websites.
- these records may be used in investigations, court proceedings or for other legal reasons.