Prairiewood High School –
ACCEPTABLE USE OF TECHNOLOGY & BYOD STUDENT AGREEMENT

Prairiewood High School supports equity and access to innovative technology to support student learning. When using their own device or prior to the authorisation of a Department of Education device, students must read and sign the Acceptable Use of Technology & BYOD Student Agreement in the company of a parent or caregiver unless otherwise directed by the principal.

I agree that I will abide by the school's Digital Devices & Online Services Policy and that I will:

Be SAFE

- □ Protect your personal information, including your name, address, school, email address, telephone number, pictures of you and other personal details.
- □ Only use your own usernames and passwords, and never share them with others.
- □ Ask a teacher or other responsible adult for help if anyone online asks for your personal information, wants to meet you or offers you money or gifts.
- □ Let a teacher or other responsible adult know immediately if you find anything online or on your phone that is suspicious,harmful, inappropriate or makes you uncomfortable.
- □ Never hack, disable or bypass any hardware or software security, including any virus protection, spam and filter settings.

Be RESPONSIBLE

- □ Follow all school rules and instructions from school staff, including when using digital devices and online services. I will only use the department's Wi-Fi network for learning and not personal use.
- □ Take care with the digital devices you use.
  - Make sure the devices you bring to school are fully charged each day and are stored appropriately when not in use.
  - Understand that you and your parents and carers are responsible for any repairs or IT support your personal devices might need.
  - Make sure the devices you bring to school have the latest software installed.
  - Take care with the school-owned devices, so that other people can use them after you. Understand that you are responsible for any damage or loss due to negligence and you will be required to pay replacement or repair costs.
- □ Use online services and mobile phones in responsible and age-appropriate ways.
  - Only use online services and phones in the ways agreed to with your teacher, when permitted for genuinely educational purposes.
  - Only access appropriate content and websites, including when using the school's filtered network and personal, unfiltered networks.
  - Do not use online services or phones to buy or sell things online, to gamble or to do anything that breaks the law.
  - Do not use any device to knowingly search for, link to, access or send anything that is: Offensive, pornographic, threatening, abusive or defamatory; or considered to be bullying, embarrassing or upsetting to another person or group.Understand the school will follow the DoE Suspension & Expulsion procedures linked to inappropriate and/or criminal behaviour. This may include Police involvement and devices or their contents may be handed to police to ensure student safety.
- □ Understand that everything done on the school's network is monitored and can be used in investigations, court proceedings or for other legal reasons.
- □ Understand that the school cannot be held responsible for any damage to, or theft of your device. However, understand that you are responsible for any damage to or theft of any school device you are borrowing.

Be RESPECTFUL

- □ Respect and protect the privacy, safety and wellbeing of others.
- □ Do not share anyone else's personal information.
- □ Get permission before you take a photo or video of someone, including from the person and from a teacher.
- □ Do not harass or bully other students, school staff or anyone, this includes cyberbullying using a digital device or online service.
- □ Do not send or share messages or content that could cause harm, including things that might be:
  - ○ inappropriate, offensive or abusive;
  - ○ upsetting or embarrassing to another person or group;
  - ○ considered bullying;
  - ○ private or confidential; and/or
  - ○ a virus or other harmful software.

□ I have read this Prairiewood HS Student Use of Technology & BYOD Student Agreement and agree to comply with the requirements

□ I have read and will abide by the NSW Department of Education **Student use of digital devices and online services policy**

Student FULL NAME: Year: ______________

Student Signature: ______________________________ Date:______________

Parent/Carer Name : ______________________________ Date: ______________

Parent/Carer Signature: ______________________________

Hardware features:

Supplied device must be a laptop with a fixed keyboard and screen; tablet devices (eg. ipads, android etc) will ***not*** be authorised.

Prairiewood High School will not accept responsibility for any issues with hardware.

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.

Operating system:

Windows 10 (preferred)

Latest version of OSX (Mac devices)

Software and apps:

Office 365 (Free to students via Department portal) Google Chrome browser.

Prairiewood High School will not accept responsibility for any issues with software.

Note: Teaching staff may request for course-specific software separately that will be at student’s expense.

Battery life:

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

RAM and Storage:

4GB memory with sufficient storage space available for school work

Ergonomics:

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

school day.

Other considerations

Casing: Tough and sturdy to avoid breakage.

Weight: Lightweight for ease of carrying.

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. Prairiewood High School will not accept responsibility for any loss orbreakage.

Back-up storage: Use of cloud services such has Google Drive or Onedrive. A portable hard drive would also be an appropriate source of back-up storage for essential documents.

For further clarification, contact our Technology Support on (02) 9725-5444 to make an appointment.

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 Acceptable Use of Technology & BYOD Student Agreement. The NSW Police may also be contacted in accordance with mandatory reporting expectations.

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.

For further clarification, contact our Technology Support on (02) 9725-5444 to make an appointment.

Access andSecurity 4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through internet and online communication services is related 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 are generally 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.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Training.
- 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.

Privacy and Confidentiality

4.2.1 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

4.2.2 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

4.2.3 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.

Monitoring, evaluation and reporting requirements

5.1 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.

5.2 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.