School Network and WiFi Acceptable Use Policy

The purpose of this document is to set out the responsibilities and acceptable use guidelines for all students using the school Network or Wifi Facilities at the Priory School.

Your access to the Service is completely at the discretion of The Priory School, and your access to the Service may be blocked, suspended, or terminated at any time for any reason including, but not limited to, violation of this Agreement, actions that may lead to liability for The Priory School or its owners, disruption of access to other Users or networks, and violation of applicable laws or regulations.

By accessing the Priory School's network you agree to abide by the following regulations during your time at the school.

- **You must not disclose your login details such as username or password to any other user unless directed to by a member of the IT Support Department.**
- You must not allow any other user to access or use any computer or device which you are logged into on the School Network.
- You must lock your computer at all times when leaving it unattended (Windows + L).
- You will maintain your own user area of 3GB in order to store any and all required school work. It is not the responsibility of the IT Support Department to ensure integrity of your user area. If you should lose work that is still required for assessment you must contact the IT Support Department immediately as they may be able to recover the data for you.
- You must not intentionally or knowingly cause damage to any IT equipment in school.
- You must not connect any device to any wireless network outside of the Student BYOD network.
- You must not create private networks through the use of tethering to a mobile hotspot.
- You must re-connect any device to the Student BYOD network each day in order to resubmit your login details for authentication in order to continue accessing the network with that device.
- You must not possess or attempt to use any software in school with the purpose of disrupting or damaging the school network.
- You must not play games using school machines during lesson times or at break and lunchtimes in any of the available computer rooms.
- You must not connect any Jailbroken or otherwise 'unlocked' devices to the school WiFi network.
- Any personal computer or laptop connected to the school wired or wireless network must be configured with antivirus software.
- You must not attempt to install and software or attempt to circumvent network installation policies.

- You must not access offensive or banned content, or use methods to subvert school network firewall filtering in order to access such content.
- You must not share offensive or inappropriate material with any other user on the school network.
- You must comply with Trademark and Copyright legislation when using IT to create work for assessment.
- You must not transmit Illegal or Copyrighted materials.
- Violation of any or all of these regulations may result in you being banned from accessing the school network for an unspecified period of time. In the event that this occurs we will also inform the Principal and Deputy Principal.