Digital Citizenship Guidelines

These guidelines have six conditions of being a Digital Citizen. The intended audience of this agreement is for Willunga High School students:

Respect Yourself.
* I will show respect for myself through my actions.
* I will select online names that are appropriate.
* I will consider the information and images that I post online.
* I will consider what personal information about my life, experiences, experimentation or relationships I post.
* I will not be obscene.

Protect Yourself.
* I will ensure that the information, images and materials I post online will not put me at risk.
* I will not publish my personal details, contact details or a schedule of my activities.
* I will report any attacks or inappropriate behaviour directed at me and I will seek support from appropriate people or organisations.
* I will protect passwords, accounts and resources.

Respect Others.
* I will show respect to others.
* I will respect my teachers by following their instructions and directions without dissent.
* I will not use electronic mediums to flame, bully, harass or stalk other people.
* I will show respect for other people in my choice of websites.
* I will not visit sites that are degrading, pornographic, racist or inappropriate.
* I will not abuse my rights of access and I will not enter other peoples’ private spaces or areas.

Protect Others.
* I will protect others by reporting abuse and by not forwarding inappropriate materials or communications or by visiting sites that are degrading, pornographic, racist or inappropriate.
* I will moderate unacceptable materials and conversations, reporting conversations that are inappropriate or unacceptable.

Respect Intellectual property.
* I will request permission to use resources. I will suitably cite any and all use of websites, books, media etc.
* I will acknowledge all primary and secondary sources.
* I will validate information.
* I will use and abide by the fair use rules.

Protect Intellectual Property.
* I will request to use the software and media others produce.
* I will use free and open source alternatives rather than pirating software.
* I will purchase, license and register all software.
* I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.
* I will report vandalism and damage. I will act with integrity.

(Andrew Churches, Educational Origami)
All students and staff have access to the Willunga High School wireless network, including the access to the National Broadband Network (NBN) Internet for teaching and learning. All users are required to acknowledge receipt and understanding of the BYOD Guidelines in this document and adhere to the Digital Citizenship Agreement, by signing the diary each year.

Violation of the WHS BYOD Guidelines while using a personal electronic device on the WHS wireless network will result in appropriate disciplinary action as specified in the Behaviour Management Policy.

**BYOD Guidelines**

1. Students may use a privately owned electronic "Internet ready" device on the WHS wireless network with teacher or administrator permission.

2. The use of a privately owned electronic device to support and enhance instructional activities is at the subject teachers’ discretion. All users of WHS wireless are bound by an acceptable use agreement whereby individuals will not over use data allowances.

3. The WHS wireless is a monitored service accessed by a unique username and password. Inappropriate sites are filtered and blocked when necessary to ensure student use of the Internet is for educational purposes.

4. Students are prohibited from accessing the Internet using any external Internet service e.g. 3G/4G devices or other alternatives.

5. No student shall establish a wireless or ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds.

6. The privately owned electronic device owner is the only person allowed to use the device and the unique username and password associated with the device. In the event that a student believes that his/her password has been compromised, he/she should immediately see IT staff to have the password changed.

7. Generally, no WHS software can be installed on personal devices due to the terms of the licenses unless stated otherwise.

8. No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.

9. Devices are brought to school at the students’ and parents’ own risk. In the event that a privately owned device is lost, stolen or damaged, WHS is not responsible for any financial or data loss, however, we will investigate any occurrence.

**SPECIFICATIONS**

**Computers:** All laptop computers will work on the network provided the device has Windows XP SP3, Windows Vista, Windows 7, Windows 8, Snow Leopard, Lion or Mountain Lion.

**Mobile Devices:** Mobile devices, such as iPads and Android Tablets will work on the network (excludes SMART phones/mobile phones).