RANDWICK BOYS' HIGH SCHOOL
BRING YOUR OWN DEVICE (BYOD)
DESIGN SPECIFICATIONS AND STUDENT RESPONSIBILITIES

CHOOSING A DEVICE

Parents will be aware of the discussion that has been occurring, through the school newsletter and parents' surveys about the Bring Your Own Device Policy of the Department of Education and Communities. Randwick Boys' High School has entered into an arrangement with a company called ASI to provide a dedicated portal for the purchase of a range of devices to suit the learning needs of our students.

While BYOD has applicability to Year 9, replacing the previous laptop rollout under the Digital Education Revolution (DER) program, BYOD opens up opportunities to all students to purchase devices, for use in education, at competitive prices.

Students should ensure that they are comfortable using their device during the school day, particularly in relation to screen size, keyboard sturdiness and other factors that might affect their capacity to use the device effectively.

The information below provides you with the requirements for any device to be able to access the school's wireless system. All devices supplied by ASI will meet the requirements of the wireless system. However, parents choosing to source devices from other suppliers should keep these specifications in mind when selecting a device.

Before being permitted to access the Department's wireless network, students and their parents or caregivers must complete the Randwick Boys' High School **Bring Your Own Device (BYOD) Student Agreement.**

Wi-Fi

The device must support dual-band Wi-Fi. There are two wireless frequencies – 2.4 GHz and 5Ghz. Older devices only support the 2.4Ghz standard, while more modern devices have dual-band Wi-Fi which adds support for 5Ghz.

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.

Student devices are only permitted to connect to the department's Wi-Fi network, while at school, at no cost.

SCREEN RESOLUTION

Minimum resolution should be tablet form-factor. The minimum size required is 1024 pixels x 768 pixels. This is the size of older tablets from iPad 2 and onwards.

PROCESSING SPEED

Tablets and Laptops that use low-power ARM and Intel Atom processors may experience performance issues and are not recommended.

OPERATING SYSTEM (OS) AND ANTI VIRUS

Windows and iOS (Apple) are strongly recommended. The operating system must be the current or one removed, no older.

The Android OS only added support for proxy-based internet with its latest version, so older devices will not connect to the Department of Education and Communities' internet. Even with the latest system, the majority of applications that access the internet have not been upgraded to include this capability, so they will still not connect to the Department of Education and Communities' internet, despite the fact the OS now supports this. We are unable to provide support for these issues at school.

Students must ensure that they have a legal and licensed version of a supported operating system and of the software they use. Student devices must be equipped with anti-virus software.

SOFTWARE

The device should have some word-processing software on it that can out put a file in a format readable by teachers on their school PC's. At the very least it should output the Rich Text Format (RTF), a cross-platform standard.

The device should have an Internet browser. All software and apps must be fully updated.

Desirable – productivity software such as MS Office (Excel and PowerPoint). In addition, some kind of simple graphics or photo-manipulation software would be useful for creating multimedia assignments.

Senior students – Specialist software as dictated by course requirements – graphics software, mathematics packages etc.

MEMORY AND RAM

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

DATA BACK UP

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

MAINTENANCE AND SUPPORT

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

PERIPHERALS

Any tablet device must have a keyboard with which it can dock. On-screen keyboards are not considered suitable for schoolwork. Tablet computers are low-powered devices that are not designed for serious content creation, such as essay writing. A virtual keyboard would be too slow for such a task.

Devices must be camera and microphone equipped.

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. Students' devices must have a minimum of 5 hours battery life to last the school day.

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 Department of Education and Communities nor Randwick Boys' High School.

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

OTHER CONSIDERATIONS AND ACCESSORIES

Casing: Tough and sturdy to avoid breakage.

Weight: Lightweight for ease of carrying.

Durability: Durable and strong.

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.

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.

RANDWICK BOYS' HIGH SCHOOL

BRING YOUR OWN DEVICE (BYOD)

ONLINE COMMUNICATION SERVICES: ACCEPTABLE USAGE FOR SCHOOL STUDENTS

Students accessing the Department of Education and Communities wireless network do so with the understanding of the following.

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 is 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.

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.

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.

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.

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.

RANDWICK BOYS' HIGH SCHOOL

BRING YOUR OWN DEVICE (BYOD)

STUDENT AGREEMENT.

Students accessing the wireless network of the Department of Education and Communities through Randwick Boys' High School do so on condition that each:

- ❒ Will use the department's Wi-Fi network for learning.
- ❒ Will use his device during school activities at the direction of the teacher.
- ❒ Will not attach any school-owned equipment to his device without the permission of the school.
- ❒ Will use his portal/internet log-in details and will never share them with others.
- ❒ Will stay safe by not giving his personal information to strangers.
- ❒ Will not hack or bypass any hardware and software security implemented by the department or school.
- ❒ Will not use his own device knowingly to search for, link to, access or send anything that is: offensive, pornographic, threatening, abusive, defamatory, or considered to be bullying.
- ❒ Will report inappropriate behaviour and inappropriate material to his teacher.
- ❒ Understands that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.
- ❒ Acknowledges that the school cannot be held responsible for any damage to, or theft of any device.
- ❒ Understands and has read the limitations of the manufacturer's warranty on his device, both in duration and in coverage.
- ❒ Has read and will abide by the Randwick Boys' High School ***Bring your Own Device (BYOD) Design Specifications and Student Responsibilities*** document.
- ❒ Has read and will abide by the NSW Department of Education and Communities' ***Online Communication Services – Acceptable Usage for School Students.***