DEPARTMENT OF EDUCATION AND COMMUNITIES

BONNYRIGG HIGH SCHOOL

Partially Selective and Local Enrolments

Principal: M N Bryce: BA (Hons)., Dip Ed., MEd

I Shall Strive for the Best

BRING YOUR OWN DEVICE

Student Contract

Student name _____ _____
Family name Given name

Parent/Carer name _____ _____
Family name Given name

……

Purpose

The Bonnyrigg High School BYOD Program aims to improve student learning experiences both in and out of the classroom. The NSW Department of Education and Communities and Bonnyrigg High School will allow students to bring a device to school on the expectation that they will make good decisions with regard to their personal use of technology.

A Student Contract must be signed and provided to the TSO before the device will be connected to the school network.

Students and parents/carers must carefully read this contract prior to signing it. Any questions should be addressed to the school and clarification obtained before the contract is signed.

BYOD Contract

We have read the BYDO Contract *(version 15.1)*.

We understand our responsibilities regarding the use of the BYOD and the school network including internet.

In signing below, we acknowledge that we understand and agree to the BYOD Contract.

We understand that we accept that the school will not be liable or take responsibility for the device if it is broken, lost and/or stolen.

We understand that failure to comply with the BYOD Contract could result in loss of access to the school network.

Signature of student: _____ date: / /

Signature of parent/carer: _____ date: / /

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

BYOD CONTRACT (version 15.1)

1. Purpose
The BYOD is to be used as a tool to assist student learning both at school and at home.

Definitions

BYOD: Bring your own device

Mobile/ digital devices
These can include, but are not limited to smart phones, laptops, tablets, and iDevices and must have up to date virus protection

2. Equipment

2.1 Ownership

2.1.1 The student must bring the BYOD fully charged to school every day. Chargers should be left at home.

2.1.2 All material on the BYOD is subject to review by school staff. If there is a police request, students must provide access to the BYOD and personal network holdings associated with the use of your BYOD.

2.2 Damage or loss of equipment

2.2.1 If you bring your own devices to school, then you accept that the school will not be liable or take responsibility for the device if it is broken, lost and/or stolen.

3. Standards for BYOD care
The student is responsible for:

i) Using their BYOD in accordance with school guidelines.

ii) Adhering to Online Communication Services: Acceptable Usage for School Students (http://bit.ly/1rJI2lW) policy.

iii) Have up to date virus protection at all times.

4. Acceptable computer and internet use

4.1 Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

4.2 Upon enrolment into a New South Wales Government school, parental/carer permission was sought to allow the student to access the Internet at school based on the *Online Communication Services: Acceptable Usage for School Students* policy. Extracts are provided below. This policy forms part of the BYOD Student Contract.

4.3 The Online Communication Services: Acceptable Usage for School Students policy applies to the use of the BYOD and internet on school grounds.

4.4 Access and Security

4.4.1 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 is generally used for genuine curriculum and educational activities whilst at school.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Communities.
- 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.

4.5 Privacy and Confidentiality

4.5.1 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.

4.6 Intellectual Property and Copyright

4.6.1 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.

4.7 Misuse and Breaches of Acceptable Usage

4.4.1 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.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

5.1.1 any internet site accessed that is considered inappropriate.

5.1.2 any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Communities.