eSmart Policy

Black Rock Primary School

Black Rock Primary School Policy Guide

Rationale

Black Rock Primary School is committed to providing a safe, secure and caring learning environment for all its students. Black Rock Primary School uses the internet and digital devices as learning tools to improve student learning outcomes by increasing access to and engagement with worldwide information. The school embraces the benefits of technology and is committed to reducing students' exposure to cyber-risks (such as cyberbullying, online sexual predation, sexting, identity theft and fraud) when using the internet, mobile phones and other electronic personal devices.
The internet and digital technologies provide many learning opportunities and are part of everyday life. While the use of digital technology is an exciting learning tool it is important for students to be responsible and safe when working in the online environment.

Aims

For Black Rock Primary School to develop a whole school approach to ensure its students are protected from bullying and cyberbullying, both while at school and when in their home environment.

The eSmart Policy should be read in conjunction with the following policy documents:

- Student ICT User Agreement
- Parent ICT User Agreement
- Staff ICT User Agreement – (upon sign-in on staff laptops)
- Bullying and Harassment Policy
- Student Engagement Policy
- ICT Acceptable Use Policy

Implementation:

All staff members are to be familiar with the above policy documents. Staff are to familiarise themselves at the beginning of each school year with each policy document and carry out the necessary requirements within their classroom and as part of their daily duties while at school.

At the beginning of each school year, and at any other time as needed, teachers are to familiarise the students with the protocols in place for using digital technologies, including both the safe handling of equipment together with the penalties imposed if incorrect use occurs.

Throughout each school year, students will receive explicit education of an eSmart curriculum in relation to:

- Staying safe online
- How to deal with conflict, bullying, cyber-bullying and harassment
- Building confidence, resilience, persistence, getting along and organisational skills
- The staff at Black Rock Primary School will use the following resources to enhance their teaching of an eSmart curriculum:
    - Friendly Schools Program
    - Student of the Week Awards
    - Incursions and excursions

Black Rock Primary School is committed to educating not only its students but also its wider community. As such, information relating to the eSmart Curriculum will be produced and distributed through school newsletters and the school website. Information sessions, which may include guest speakers, will be made available to the wider school community at times which will be advertised through the relevant communication channels.

All students will annually sign a Student ICT User Agreement.

All staff members are responsible for ensuring that students adhere to the Student User Agreements. Any breaches of this agreement will be documented, and appropriate consequences will be set in line with the school's ICT Acceptable Use Policy.

The use of digital devices are a part of everyday learning at Black Rock Primary School. Students are expected to adhere to the Black Rock Primary School ICT Acceptable Use Policy.

In line with the Bullying and Harassment Policy, all students and staff are responsible for reporting any form of bullying (including cyber-bullying) or harassment to either a teacher or the Student Welfare Coordinator. The teacher or Student Welfare Coordinator will follow the procedures as set out in the abovementioned policy document.

The school community as a whole has a responsibility for the safety of the students at Black Rock Primary School and as such, parents, caregivers and others who witness any form of conflict, bullying (including cyber-bullying) or harassment are expected to report this to the Student Welfare Coordinator as soon as is practicable.

<u>Authorised Usage and eSmart Agreement:</u>

- As the school provides network access, the contents of the school ICT system, including email messages, remain the property of the DET. The school has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.
- All users, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices, will be issued with this Agreement.
- The school's ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the Student ICT User Agreement has been signed and returned to the student's class teacher. Signed Agreements will be filed in a secure place.
- The school encourages anyone with a query about these guidelines or the Agreement to contact your child's class teacher in the first instance.

<u>Obligations and requirements regarding appropriate use of ICT in the school learning environment:</u>

- While at school, using school owned or personal ICT equipment/devices is for educational purposes only.
- When using school or privately owned ICT on the school site or at any school related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:
  - Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism, or is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing.
  - Has intention to deceive, impersonate or misrepresent.
  - Forwards confidential messages to persons to whom transmission was never authorised by the school, including persons within the school community and persons/organisations outside the school community.
  - Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus.
  - Breaches copyright.
  - Attempts to breach security and infrastructure that is in place to protect user safety and privacy.
  - Results in unauthorised external administration access to the school's electronic communication.
  - Propagates chain emails or uses groups or lists inappropriately to disseminate information.
  - Inhibits the user's ability to perform their duties productively and without unnecessary interruption.
  - Interferes with the ability of others to conduct the business of the school.
  - Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices.

- Involves the unauthorised installation and/or downloading of non-school endorsed software.
- Breaches the ethos and values of the school.
- Is illegal.

- In the event of accidental access of such material, Authorised Users must:
  - Not show others.
  - Shut down, close or minimise the window.
  - Report the incident immediately to the supervising teacher.

- A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of school, or privately owned communication technologies, on the school site or at any school related activity, may also be found to have engaged in prohibited use.
- While at the school or a school-related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the school site, or to any school related activity such as USB sticks.
- Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. Any Authorised Users with a query or a concern about that issue must speak with the relevant class teacher or subject teacher.

Monitoring by the School – The school reserves the right to:

- at any time check work or data on the school's computer network, email, internet, computers and other school ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.
- at any time check work or data on privately owned ICT equipment on the school site or at any school related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise cooperate with the school in the process. Before commencing the check, the school will inform the Authorised User of the purpose of the check.
- Have an electronic access monitoring system, through eduSTAR (in accordance with DET requirements), which has the capability to restrict access to certain sites and data.
- Monitor traffic and material sent and received using the school's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.
- From time to time conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit of content and usage.

Copyright, Licensing, and Publication

- Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.
- All material submitted for internal publication must be appropriate to the school environment and copyright laws.
- Any student/s found to use an ICT equipment/device to gain advantage in exams or assessments will face disciplinary actions as sanctioned by the school.

Individual password logons to user accounts

- If access is required to the school computer network, computers and internet access using school facilities, it is necessary to obtain a user account from the school.
- Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.
- Authorised Users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other school ICT equipment/devices can be traced by means of this login information.

- Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Guidelines and Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the school environment.
- For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

Other Authorised User obligations

- Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.
- Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.
- Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

Privacy

- School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the school's privacy agreement or with proper authorisation. The Privacy Act requires the school to take reasonable steps to protect the personal information that is held by the school from misuse and unauthorised access. Authorised users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.
- While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the public standing of the school may result in disciplinary action. The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, Instagram, YouTube, Tumblr (and any further new technology).

Procedures for Mobile Phone Use at School

Black Rock Primary School accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on school property and during school excursions and camps, use of mobile phones is not permitted during school hours unless authorised by a school staff member.

Responsibility

- It is the responsibility of students who do bring mobile phones or personal electronic devices onto school premises to adhere to the guidelines outlined in this document and the eSmart Student Acceptable Use Agreement.
- Students are required to mark their mobile phone or personal electronic device clearly with their name.
- Mobile phones must remain on silent during class times and be kept in school bags for the duration of the day (unless student is given permission from a staff member).
- Mobile phones must not be used during school hours unless permitted by a staff member.
- The school accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.
- The school accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from school.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.
- Students must protect the privacy and dignity of individuals and security of information, to maintain the public standing of the school and compliance with State and Federal laws.

- The school strongly advises that for safety reasons headphones should not be used when students are traveling to and from school, eg. walking, riding a bike, moving on and off buses.
- In accordance with school policies, any unauthorised mobile phone or personal electronic device being used during the school day will be confiscated. Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made with a staff member.

Procedures for BYO iPads (Applicable to Year 5/6 Students)

- During the time that the iPad is at school, it is to be used by students for educational purposes. Students are responsible for all information and content on the device, which needs to fit within the eSmart Student Acceptable Agreement guidelines.
- The students should come to school each day with their iPad fully charged for the day's activities.
- The use of privately owned iPads while at school will follow the same regulations as applies to our existing school iPads. They are only to be used for tasks relating to school work, and consequences will result from any inappropriate use, as determined by the student's supervising teacher at the time.
- Teaching staff reserve the right to look at any application, file, or browsing history data on the iPad at any time.
- The iPad must not be left sitting on the ground, on a chair or left outdoors at any time. The iPad should be left on tables, stored in tubs or in teachers' locked cabinets when not in direct use.
- iPads will be put away at eating times. No food or drink should be consumed near student iPads.
- They will not be taken outside without the direct permission and supervision of a teacher either during class time, recess or lunchtime.
- When travelling to and from school, the iPad should remain in a zipped up school bag. Students are strongly advised not to use the iPad between school and home. This also applies once students are on school grounds before and after school.
- The school recommends that when using the iPad at home it is used at all times in a family or common area and not in the student's bedroom or other private space unsupervised.
- Device must be configured so that educational/school use apps are on the front screen of the device. Other apps e.g. games (should they be present on the device) are to be on the 2nd screen in a single folder. These must not be accessed at school
- Students must ensure there is adequate storage space on the device to allow for school related tasks to be completed and apps to be downloaded while at school.
- iPads must be kept in a protective case, which is to remain on the iPad at all times while at school. Screen protectors are strongly advised.

Evaluation

This policy will be reviewed as part of the school's three-year review cycle or sooner as updates to technology and associated platforms require.

This policy was last ratified by School Council in…	July 2017