eSmart policy

Policy

Bunyip Primary School (Bunyip PS) uses the Internet as a learning tool to improve student learning outcomes by increasing access to 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 and other electronic personal devices. This policy should be read in conjunction with the 'Bunyip PS eSmart Use of ICT Guidelines' (attached to this policy).

Purpose

The aim of the policy is to:

- Establish an eSmart culture which is in keeping with the values of the school and the expectations outlined in the Bunyip PS 'eSmart Use of ICT Guidelines' and the Bunyip PS Student Engagement Policy/Student Code of Conduct which includes actions and consequences for inappropriate behaviour.
- Educate Bunyip PS students to be smart, safe, responsible and ethical users of digital technologies.
- Recognise that explicitly teaching students about safe and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school.
- Achieve accreditation as an eSmart school by meeting all criteria as outlined in the eSmart System Tools.

Implementation

1. Bunyip PS staff are trained in the philosophies of the eSmart program and are provided with the information necessary for cyber-safety education.
2. All Bunyip PS students will undertake a cyber-safe program and will be required with their parents to sign an eSmart ICT Acceptable Use Agreement before they will be permitted to use any information and communications technology (ICT) at school.
3. The school community will be provided with cyber-safety information on a regular basis.
4. Safe and responsible online behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home.
5. Bunyip PS staff will raise student awareness of issues such as online privacy and intellectual property including copyright, and that some online activities are illegal and will be reported to police.
6. Bunyip PS staff will supervise students when using digital technologies for educational purposes and provide a filtered internet service whilst acknowledging that full protection from inappropriate content can never be guaranteed.
7. Mobile phones and other personal electronic devices may only be brought to school with prior permission of the Principal. Parents and students must comply with the conditions of use as outlined in Section 8 of the Bunyip PS 'eSmart Use of ICT Guidelines', which prohibits students from accessing mobile phones and other personal electronic devices within the school grounds.

8. Bunyip PS staff will immediately respond to issues or incidents that have the potential to impact on the wellbeing of our students.
9. All incidents of cyberbullying must be referred to the Principal or classroom teacher for investigation and any action taken will be in line with the Student Engagement Policy/Student Code of Conduct.
10. Parents will be notified and expected to meet with school staff if students are involved in any incidents of cyberbullying.
11. Students are advised to report an incident to their teacher immediately if:
    - They have experienced an incident of cyberbullying.
    - They feel the welfare of other students at the school is being threatened.
    - They come across sites which are not suitable for our school.
    - Someone writes something they don't like, makes them or their friends feel uncomfortable or asks them to provide private information.
    - They accidentally do something which is against the rules and responsibilities they have agreed to.
12. Any student who does not follow the rules of the eSmart Policy, acceptable use agreement and the Bunyip PS eSmart Use of ICT Guidelines will lose their ICT privileges (for a length of time as deemed appropriate by the Principal) and be required to complete additional cyber-safety lessons before their privileges are returned.. .
13. The eSmart Policy also applies during school excursions, camps and extra –curricular activities.

Ratified by School Council November 2017

Review Date: November 2018

eSmart use of ICT guidelines

User eSmart obligations

1. **Authorised usage and eSmart agreement**
   1.1. As the school provides network access, the contents of the school ICT system, including email messages, remain the property of the DEECD. 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.
   1.2. 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 the acceptable use agreement. This document should be read carefully with the acknowledgement page signed and returned to the student's class teacher.
   1.3. The school's ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of the acceptable use agreement has been signed and returned to the student's class teacher. Signed agreements will be filed in a secure place.
   1.4. The school encourages anyone with a query about these guidelines or the acceptable use agreement to contact your child's class teacher in the first instance.

2. **Obligations and requirements regarding appropriate use of ICT in the school learning environment**
   2.1. While at school, using school owned or personal ICT equipment/devices is for educational purposes only.
   2.2. 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:
      2.2.1. Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism, is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing; has intention to deceive, impersonate or misrepresent;
      2.2.2. 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
      2.2.3. Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
      2.2.4. Breaches copyright
      2.2.5. Attempts to breach security and infrastructure that is in place to protect user safety and privacy
      2.2.6. Results in unauthorised external administration access to the school's electronic communication
      2.2.7. Propagates chain emails or uses groups or lists inappropriately to disseminate information
      2.2.8. Inhibits the user's ability to perform their duties productively and without unnecessary interruption,

2.2.9. Interferes with the ability of others to conduct the business of the school
2.2.10. Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices.
2.2.11. Involves the unauthorised installation and/or downloading of non-school endorsed software
2.2.12. Breaches the ethos and values of the school
2.2.13. Is illegal

2.3. In the event of accidental access of such material, authorised users must:
2.3.1. Not show others
2.3.2. Shut down, close or minimise the window
2.3.3. Report the incident immediately to the supervising teacher.

2.4. A person who encourages, participates or otherwise knowingly undertakes 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.

2.5. 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.

2.6. Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any authorised users with a query or a concern about that issue must speak with the relevant class teacher or subject teacher.

3. Monitoring by the school

3.1. The school:

- reserves the right at any time to 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.
- reserves the right at any time to 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 co-operate with the school in the process. Before commencing the check, the school will inform the Authorised User of the purpose of the check.
- has an electronic access monitoring system, through Netspace (in accordance with DEECD requirements), which has the capability to restrict access to certain sites and data.
- monitors 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.

4. **Copyright, licensing, and publication**
   4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged.
   4.2. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.
   4.3. All material submitted for internal publication must be appropriate to the school environment and copyright laws.
   4.4. 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.

5. **Individual password logons to user accounts**
   5.1. 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.
   5.2. 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.
   5.3. 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.
   5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with these guidelines and the acceptable use 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.
   5.5. 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.

6. **Other authorised user obligations**
   6.1. Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.
   6.2. 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.
   6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

7. **Privacy**
   7.1. 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.
   7.2. 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 or staff will result in disciplinary action.
   7.3. The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, YouTube, Tumblr (and any further new technology).

8. **Procedures for mobile phone and other electronic device use at school**
   8.1. It is the preference of the school that mobile phones and personal electronic devices are not to be brought to school; however Bunyip PS accepts that some parents provide their children with mobile phones and other personal electronic devices.
   8.2. Whilst at school the device must be handed to the classroom teacher at the start of the school day (8.50am). It will be returned to the student at the end of the school day
   8.3. Mobile phones and electronic devices are not permitted on excursions or camps (as per the Camps and Excursions Policy).

Responsibility

- Parents must seek permission from the Principal prior to any phone or device being brought to school by a student.
- If a student is permitted to bring a mobile phone or personal electronic device onto school premises must hand the device to the classroom teacher at the start of the school day (8.50am). It is the student's responsibility to take care of the device until such time as it is passed over to the teacher. It will be returned to the student at the end of the school day.
- **Students are to switch off their phone or personal electronic device when they enter the school grounds and cannot turn it back on until they have left the school grounds.**
- Failure to comply with the above requirements will result in the phone or personal electronic device being removed from the student and the parent will have to meet with principal before it can be collected
- 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.
- Students must keep their password/pin numbers confidential.
- 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.

- It is the schools responsibility to ensure that in the case of an emergency, the school office remains a vital and appropriate point of contact. This will ensure your child is reached quickly, and assisted in the appropriate way

Breach of guidelines

Breaches of these guidelines will be dealt with in accordance with the school Student Engagement Policy.