e-Learning Policy

1. Scope

1.1 The Coatesville Primary School eLearning Policy addresses three broad areas:

1.1.1 access and management of ICT equipment;

1.1.2 access to the internet; and

1.1.3 e-Smart practices.

2. Definitions

2.1 **Agreement** - Student e-Learning Agreement.

2.2 **Authorised User** - a student who has signed the Agreement (or has had it signed by a parent) and is authorised by the school to use school ICT.

2.3 **DET** – Department of Education and Training.

2.4 **e-Smart** – refers to the name of the cyber safety guidelines that are followed at Coatesville Primary School to promote the safe, responsible and ethical use of ICT.

2.5 **Educational purposes** – activities that are linked to curriculum related learning or student engagement activities.

2.6 **IB –PYP** - International Baccalaureate – Primary Years Programme.

2.7 **ICT** – Information and Communications Technology.

2.8 **ICT equipment** - includes, but is not limited to, communication made using ICT equipment/devices such as PCs, laptops, tablets, internet, email, instant messaging, online discussions/surveys, mobile phone activities and related applications.

2.9 **Leadership Team** - consists of Principal, Assistant Principal and Leading Teachers.

2.10 **Unacceptable student conduct' or 'inappropriate use** - includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.

3. Rationale

3.1 Coatesville Primary School recognises that teaching and learning will change as information and telecommunication technologies alter the ways in which information is accessed, communicated and transferred. Consequently, electronic information research skills are now essential for students as members of our society and as future employees. In responding to these changes, the school actively supports access by students to the widest variety of information resources, together with the development by staff of appropriate skills to analyse and evaluate such resources.

4. Purpose

4.1 Our aim is to provide an educative environment by establishing an e-Smart culture in keeping with the values of the school, legislative and professional obligations and the community's expectations. Within this context, the objective of this Policy is to ensure the smart, safe and responsible use of ICT within the school community.

4.2 This Policy and the Agreement outlines the conditions for the use of all school ICT and behaviours associated with safe, responsible and ethical use of technology. Authorised Users are required to comply with the Agreement.

5. Student User e-Smart Obligations

Authorised Usage and the Agreement

5.1 As the school provides network access, the contents of the school ICT system, including email messages, remains the property of the DET. The school has the capability to monitor and control the ICT system and reserves the right to monitor individual usage and report, where necessary, any actual or suspected misconduct or prohibited use.

5.2 All student 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 Agreement. This document should be read carefully with a parent/carer and the acknowledgement page signed and returned to the student's class teacher.

5.3 The school's ICT, including network facilities, communication technologies and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed by a parent/carer and returned to the student's class teacher. Signed Agreements will be filed in a secure place.

5.4 The school encourages anyone with a query about the e-Smart Policy and e-Learning Agreement to contact their child's class teacher in the first instance.

Obligations and requirements regarding appropriate use of ICT in the school learning environment

5.5 The use of school owned ICT equipment by students is for educational purposes only.

5.6 When using school or privately owned ICT on the school premises or at any school related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate. Examples include (but are not limited to):

5.6.1 would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism or sexism;

5.6.2 is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening or harassing;

5.6.3 has the intention to deceive, impersonate or misrepresent;

5.6.4 forwards confidential messages to persons to whom transmission was not authorised by the school, including persons within the school community and persons/organisations outside the school community;

5.6.5 fails to use the system as prescribed, thus permitting accidental or deliberate infection by a computer virus;

5.6.6 breaches copyright;

5.6.7 attempts to breach security and infrastructure that is in place to protect user safety and privacy;

5.6.8 results in unauthorised external administration access to the school's electronic communication;

5.6.9 propagates chain emails or uses groups or lists inappropriately to disseminate information;

5.6.10 inhibits the user's ability to perform their duties productively and without unnecessary interruption;

5.6.11 interferes with the ability of others to conduct the business of the school;

5.6.12 involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices;

5.6.13 involves the unauthorised installation and/or downloading of non-school endorsed software; and

5.6.14 breaches the ethos and values of the school.

5.7 In the event of accidental access of such material, Authorised Users must:

5.7.1 not show it to others;

5.7.2 shut down, close or minimise the window; and

5.7.3 report the incident immediately to the supervising teacher.

5.8 A person who encourages, participates or otherwise knowingly agrees to the 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.

5.9 While at the school or a school related activity, Authorised Users must not have any 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.

5.10 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 an issue must speak with the relevant supervising teacher.

6. Monitoring by the School

The school:

6.1 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;

6.2 reserves the right at any time to check work or data on privately owned ICT equipment on the school premises 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;

6.3 has an electronic access monitoring system through Netspace (in accordance with DET requirements), which has the capability to restrict access to certain sites and data;

6.4 monitors traffic and material sent and received using the school's ICT infrastructures. This may be analysed and monitored, from time to time, to help maintain an e-Smart learning environment; and

6.5 will, 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.

7. Copyright, Licensing, and Publication

7.1 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 and images.

7.2 All material submitted for internal publication must be appropriate to the school environment and copyright laws.

7.3 Any student/s found to use an ICT equipment/device to gain unfair advantage in assessments will face disciplinary action as sanctioned by the school.

8. Implementation

8.1 An e-Learning Coordinator will be appointed annually to oversee the program in consultation with the Leadership Team.

8.2 The e-Learning Coordinator will oversee the coordination and implementation of the Policy and Agreement in each grade level.

8.3 Teachers collaborate with the e-Learning Coordinator and within their grade team to develop and implement ICT learning experiences that will be integrated into the curriculum.

8.4 Teachers will address and constantly refer to the e-Learning Policy and the Agreement within their class and ensure that they are abided.

8.5 Teachers will refer to the Positive Behaviours Model when dealing with student behaviours that do not abide by the Agreement.

9. Individual password logons to user accounts

9.1 If access to the school computer network, computers and internet using school facilities is required it is necessary to obtain a user account from the school.

9.2 Authorised Users must keep usernames and passwords confidential and not share them with other students. A breach of this rule could lead to Authorised Users being denied access to the system.

9.3 Authorised Users must not allow other students access to any ICT equipment logged in under their own user account. Material accessed on a student user account is the responsibility of that student. Any inappropriate or illegal use of the computer facilities and other school ICT equipment can be traced by means of this login information.

9.4 Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Policy and the 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.

9.5 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.

10. Other Authorised User obligations

10.1 Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

10.2 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.

10.3 Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

11. Privacy

11.1 School ICT and electronic communication should never be used to disclose personal information of another student 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.

11.2 While after school use of communication technologies by students is the responsibility of parents/carers, 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 without permission. 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, YouTube, Tumblr (and any other platform).

12. Procedures for Mobile Phone Use at School

12.1 It is the preference of the school that mobile phones are not brought to school.

12.2 Coatesville Primary School accepts that some parents provide their children with mobile phones. However, during teaching hours (9.00am-3:30pm), use of mobile phones is not permitted unless authorised by the Principal or Assistant Principal.

13. Responsibility for Mobile Phones at School

13.1 It is the responsibility of students who do bring mobile phones onto school premises to adhere to this Policy.

13.2 The decision to provide a mobile phone to their children is the responsibility of parents/ carers.

13.3 If a child takes a mobile phone onto school premises the child's parent/carer must advise the child's class teacher that the child has their permission to have the mobile phone at school.

13.4 Students must switch off their mobile phone and place it in the designated mobile phone storage unit in their class.

13.5 Students are required to mark their mobile phone clearly with their name.

13.6 The school accepts no responsibility for replacing lost, stolen or damaged mobile phones. Their safety and security is wholly in the hands of the student.

13.7 The school accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from school.

13.8 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 must not be shared.

13.9 In accordance with school policies, any mobile phone being used inappropriately during the school day will be confiscated.

14 Safety

14.1 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.

14.2 The school strongly advises that for safety reasons headphones should not be used when students are traveling to and from school, e.g. walking, riding a bike, moving on and off buses.

15 Social Media

15.1 The school does not condone use of social networking sites which are not age appropriate, such as Facebook.

15.2 The school does not condone and is not responsible for students creating social media accounts outside of the school environment.

15.3 Students must abide by the guidelines set in the Social Media Policy.

15.4 A breach of the Social Media Policy will be considered by the Principal and the Leadership Team and will be dealt with on a case by case basis.

15.5 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 by students to parents during school hours are to be made with a staff member.

16 Breach of Agreement

16.1 Breaches of the Agreement will be dealt with in accordance with the school Student Engagement, Well-being & Inclusion Policy.

17 Evaluation

17.1 The policy will be reviewed annually in line with the school's review cycle.

This policy was last ratified by School Council on 22nd August 2017