WESTGROVE PRIMARY SCHOOL

eSmart POLICY

At Westgrove Primary School we hold the care, safety and wellbeing of children as a central and fundamental responsibility of our school. Our commitment is drawn from our School Vision and Values statements as outlined in our Student Engagement and Inclusion Policy.

Purpose:

This Policy outlines the conditions applying to the use of all school Information Communication Technologies and behaviours associated with safe, responsible and ethical use of technology and online environments.

Rationale:

The School aims to provide an eSmart culture within the educative environment which is in keeping with the values of the School, legislative and professional obligations, and the community's expectation.

Aim:

The aim of this Policy is to ensure the smart, safe, responsible use of ICT within the school community. To keep students safe from harm, including all forms of abuse in all school environments, online and in other locations provided by the school.

This policy should be read in conjunction with the Student Engagement and Inclusion Policy, the Mobile Device Policy and the School Staff Social Media Policy. This Policy upholds and builds upon the conditions of the student Acceptable User Agreements.

eSmart Guidelines:

1. Authorised Usage.

- as the school provides network access, the contents of the school ICT system remain the property of the school
- the school controls the system and monitors individual usage and will report, where necessary, any misconduct or prohibited use
- the school's ICT, including network facilities, communication technologies, eLearning tools and ICT equipment/devices all fall under this policy. The use of personal ICT and communication devices fall under this policy when used for the purpose of communicating about school community members

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

- while on the school grounds, the use of school owned or personal equipment/devices, is for educational purposes only
- when using any ICT device in our school environment, online and in any other locations provided by the school, prohibited use includes, ***but is not limited to,*** any conduct that is defined as objectionable and inappropriate. Refer to the Mobile Device Policy for further details
- if there is accidental access to objectionable or inappropriate material, Users must: not show others, shut down, close or minimise the window, report the incident immediately to the supervising teacher
- it is prohibited for a person to encourage, participate or otherwise knowingly be involved in prohibited use of school, or privately owned communication technologies, within all school environments or at any school related activity.

- while at school or on a school related activity, Users must not have involvement with any material which might place them at risk or breaches of the eSmart Policy. This includes images or material stored on privately owned ICT equipment/devices brought onto the school grounds or to any school related activity, for example, a USB stick.
- users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment that breaches the eSmart Policy, or use such software/hardware.

When using a digital device with a camera:

- the taking of photos and recording sound or video can only be carried out with the permission of the teacher when it is part of a class or lesson.
- all Users must be respectful in the photos taken or video captured and never use these as a tool for bullying.

3. Copyright, Licensing, and Publication.

- copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Users must not breach laws of copyright, moral right or intellectual property. This includes illegal copies of software, music, videos and images.
- do not publish any image or video taken at the school or of any student in school uniform without the written permission of the Principal.

4. Individual password logons to user accounts

It is the responsibility of all Users to ensure that no electronic communications cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or predatory conduct designed to prepare or 'groom' a child or in any other way be inappropriate in the school environment. Students must keep usernames and passwords confidential and not share them with anyone else. Students must not allow another person access to any equipment/device logged in under their own user account. Misuse could lead to students being denied access to the system.

- it is the responsibility of each User to ensure they do not download or access inappropriate or illegal material. Inappropriate use can be traced by login information and offenders will be denied access.
- those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Policy.
- for Privacy laws and personal safety, students must not reveal personal information about themselves or others. Personal information may include, but is not limited to, home or email addresses, and any telephone numbers, including mobile numbers.

5. Privacy

- 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. Students must take responsibility for the security of their computer and not allow it to be used by others.
- 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 without specific permission from Westgrove Primary School.

***Inappropriate Behaviour*:**

Failure to follow this Policy can undermine the values of Westgrove Primary School and the safety of the eLearning environment. Behaviours that are deemed by the school to be harmful to the safety of individuals or the school may result in actions such as:

- Withdrawal of access to the school network and devices.

- Confiscation of personal devices used inappropriately throughout the school day, and collected by the student or parent at a later time, determined by the Principal (including all excursions and camps).
- Suspension in cases of serious misconduct.
- It is a criminal offence to use an ICT device to menace, harass, make threats, or offend another person. In these instances, the school may consider it appropriate to involve police. Devices believed to contain evidence of a criminal act may be held and handed to Police for evidence.

Related School Policies

- Child Safe Policy

Evaluation:

This Policy was last ratified by School Council on: 11th October 2016

This Policy will be reviewed as part of the school's three-year review cycle in 2019 or where necessary due to changes in regulations or circumstances.