Glamorgan School

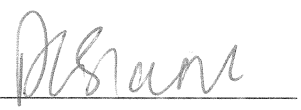
Cyber Safety Policy

Rationale

To maximise the educational benefits of existing and developing communication technologies while minimising the risks, in order to meet the school's statutory obligations to maintain a safe learning environment.

Guidelines

1. Students and parents/caregivers are given a Cyber Safety Use Agreement to read and sign. These forms are completed at Year 1 and at Year 4 or upon enrolment to the school. These forms outline the regulations and conditions under which computers and communication technologies may be used while at school or in any way which affects the safety of the school learning environment.
2. Students will be supervised while using the Internet.
3. All staff must sign the Responsible Use Agreement which includes details of their professional responsibilities and the limits to their own use of the Internet and relevant supplied technology e.g. laptops.
4. Visitors, including student teachers, may be allocated a guest login and password if necessary, to the school network.
5. Educational material on cyber safety will be provided by management to staff and students, and if requested to parents/caregivers. Safety education will be delivered, where relevant, through teaching programmes. In addition, school rules pertaining to computer use must be displayed by classroom computers.
6. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the school's computer/s and/or network facilities at any time.
7. Ongoing training for staff will be made available by management, as will appropriate professional development.
8. All necessary procedures will be put into place by the school to address cyber safety issues in all venues where the Internet and other communication technologies are accessed by staff or students.
9. The school will provide an electronic security system (filtering, monitoring, firewalling etc.), which is financially practicable. The school will continue to refine methods to improve cyber safety.
10. A Cyber Safety Officer (CO) will be appointed and will be responsible for the establishment and maintenance of a cyber safety programme in the school. The CO will be the main point of contact for all issues or incidents involving communication technologies in the school, and will report to the Principal.
11. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1993.
12. The Board supports the right of the school to check communication technology-related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches of the school's cyber safety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the Police or any other relevant authority or agency.

Signed  Date 30th May 2019

Review Date: May 2022