CYBERSAFETY POLICY

Rationale:

St Gregory the Great Catholic Primary School commits to providing a safe and nurturing culture for all children and young people in Catholic schools and will comply with the Ministerial Order No. 870-Child Safe Standards - Managing the risk of child abuse in schools

At St Gregory the Great Primary School we promote the value of respect (we are considerate of others and recognise their worth as individuals) in an environment which is physically, socially and emotionally secure and safe. The measures to ensure the cybersafety of the school environment are based on this core value. The school's information technologies provide exciting learning opportunities to expand the teaching and learning programs at St Gregory's School and are vital to the effective operation of the school. However, it is essential that the school support the secure, safe and responsible use of ICT equipment/digital devices through the education of students and preventative measures. Therefore, St Gregory's School has cybersafety practices in place, which include the eSmart program, ICT user agreements for all students, teacher and parent protocols and classroom cybersafety statements. The overall goal of the school is to help keep the students cybersafe by creating and maintaining a cybersafety culture which is in keeping with the values of the school, as well as legislative, and professional obligations.

Definition:

Cyberbullying

Cyberbullying is a term used to describe bullying that is carried out through digital technologies. It is often combined with off-line bullying. It may include a combination of behaviours such as pranking (i.e. hang up calls) sending insulting text messages, publishing someone's private information, creating hate sites or implementing social exclusion campaigns in social networking site uses technology to run a multi-steps. It is also cyberbullying when a student(s), uses technology to run a multi-step campaign to bully another student, e.g. setting another student up to be assaulted, video-recording their humiliation, posting the video-recording online and then sending the website address to others.

CYBERSAFETY POLICY

Aims:

- To develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and digital devices/equipment of flexible student learning and for the effective operation of the school, while minimising and managing any risks.
- To address the need of students and other members of the school community in receiving education about the secure, safe and responsible use of present and developing information and communication technologies.
- To ensure that all reported incidents of cyberbullying are investigated appropriately and that support is given to both victims and perpetrators.

Implementation:

- All students will be issued with a user agreement via Caremonkey. Parents are required to read these pages carefully with a signed response
- Staff are issued with teacher ICT protocols and are required to read these carefully and adhere to these requests to demonstrate best practice for the school and its students.
- All classes are required to develop a personalised cybersafety classroom statement at the beginning of each year, which includes information on obligations and responsibilities that undermine the purpose and safety of using ICT at school.
- The use of the school computer network, Internet access facilities, computers and other ICT equipment/devices by staff and students is limited to educational, professional development, and personal usage appropriate in the school environment, as defined in the student user agreements and staff protocols. St Gregory's Primary School has the right to monitor, access, and review all these uses.
- No individual may use the school internet facilities and school-owned ICT devices/equipment in any circumstances unless the appropriate user agreement has received a signed response. User agreements also apply to the use of privately-owned ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned equipment.
- Students who bring any device to school are not permitted to bring them in to class. They are required to sign the device into the office each morning and collect it at the end of the school day.
- The school and its provider takes all reasonable precautions within our control to screen material being accessed through information systems such as the internet. The school monitors traffic and material sent and received using the school's ICT infrastructures. This may be examined and analysed to help maintain a cyber safe school environment when the need arises.
- The user agreements are also an educative tool and should be used as a resource for the professional development of staff as well as the on-going education of the students in matters pertaining to this area.

- The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites such as social networking and web based email (Facebook, Twitter etc).
- Users must not attempt to circumvent monitoring or filtering.
- The user agreements operate in conjunction with other cybersafety initiatives, such as cybersafety education (ACMA, BUDDIE) supplied to the school community. This education plays a significant role in the school's overall cybersafety program, helping students to be cyber safe in all areas of their lives.
- All staff and students will be expected to communicate appropriately in a range of social contexts and take responsibility for self when communicating with others.

Breaches of the user agreement/protocols

The safety of children is of paramount concern. Breaches of the user agreement can undermine the values of the school and the safety of the learning environment, especially when ICT/digital devices are used to facilitate misconduct. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cybersafety practices. Such a breach which is deemed harmful to the safety of the school (for example, inappropriate use, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the user agreement in an appropriate manner, taking into account all relevant factors on a case by case situation.

School responses to breaches may include one or more of the following:

- a discussion with the student
- informing of, and meeting with parents
- loss of ICT privileges
- for a given period of time students may be required to complete activities relating to the safe use of technology
- the cost of ICT repairs or replacement may be incurred by the family
- action to be enforced as outlined within the behaviour management policy.

If there is a suspected breach of user agreement involving privately-owned ICT e.g. USB flash drive on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

Involvement with material which is deemed inappropriate in a school setting is a very serious matter, which may constitute criminal misconduct, such as cyber bullying. In such situations advice will be sought from an appropriate source, such as ACMA (Australian Communications and Media Authority) and the eSafety Commissioner. Parents will be contacted and it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.

CYBERSAFETY POLICY

Evaluation:

This policy will be reviewed annually as part of the school's four year review cycle.

Date of review	Term 4 2019
Developed by	St. Gregory the Great Catholic Primary School Leadership Team and Staff
Date of next review	Term 4 2020