

Doncaster Gardens Primary School Online Safety Policy

Philosophical Basis:

Doncaster Gardens Primary School has an obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. These responsibilities are increasingly being linked to the use of the Internet and Information and Communication Technologies (ICTs), and related Internet safety issues. The use of the Internet and ICT equipment bring great benefits to the teaching and learning programs, and the effective operation of the school. However, it is recognised that the presence in the learning environment of these technologies, some provided by the school and some used by staff, students, and families outside the school, can also facilitate anti-social, inappropriate and even illegal materials and activities. The school has the dual responsibility of maximising the benefits of new technologies, whilst minimising the risks. Safe online practices will aim not only to maintain a safe school environment, but also to educate students and other members of the school community about the safe and responsible use of present and developing ICTs. The prevention of cyberbullying is a priority for the school. Cyberbullying is the use of technology to bully a person or a group with the intent to hurt them socially, psychologically or even physically. It can be verbal, written or with the use of imagery using the various media available.

Cyberbullying can occur in many ways, including:

- abusive texts and emails
- hurtful messages, images or videos
- imitating others online
- excluding others online
- humiliating others online
- nasty online gossip and chat

Guidelines:

The following issues will be considered:

- The need for ongoing funding for safe Internet practices through inclusion in the school's annual budget
- Review of the Schools Strategic Plan and Annual Implementation Plan to ensure they make provision for safe Internet practices
- Deployment of staff to appropriate positions in regard to their knowledge of ICTs and safe Internet practices
- Professional learning and training for all staff in safe Internet practices
- Implications for the design and delivery of the curriculum
- Disciplinary responses appropriate to the breaches of Internet safety
- Availability of appropriate support for victims of online bullying

Implementation:

- The school's safe Internet practices will be based on the latest information available, including any initiatives endorsed by the DET.
- No individual may use the school Internet facilities and school owned/leased ICT devices/equipment in any circumstances unless the appropriate acceptable use agreement has been signed and returned to the school. Acceptable use agreements also apply to the use of privately owned/leased ICT devices/equipment on the school site, or at/for any school related activity of its location. This includes off site access to the school network from school or privately owned/leased equipment.
- The acceptable use agreements will cover all School Councillors, staff, students and any other individuals authorised to make use of the school's Internet facilities, including pre-service teachers, external providers and contractors, and other special visitors to the school.
- The acceptable use agreements are also an educative tool and can be used as a resource for the professional learning of staff.
- Signed acceptable use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.

- Use of the internet and the ICT devices/equipment by staff, students and other approved users is to be limited to educational, professional learning and personal usage appropriate in the school environment.
- The school has the right to monitor, access and review all use. This includes personal emails sent and received on school computers and/or network facilities at all times.
- The school has the right to audit at any time any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
- Issues relating to confidentiality, such as viewing 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 *Information Privacy Act 2000*.
- The safety of the students is of paramount concern. Any apparent breach of online safety will be taken seriously. The response to individual incidents will follow the procedures set out in the Student Code of Conduct and the Internet Policy and Code of Practice. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.
- For the BYOD program, students are required to install monitoring software.
- Any incidents relating to the BYOD program may result in that device being confiscated and the parents notified.
- If a device is found to be in breach of the DGPS ICT policies, the device will be confiscated and the parents notified.
- DGPS is not responsible for the creation or use of social media groups/sites used by the school community such as 'Whats App' and any information provided by parents is volunteered.

Evaluation:

- This policy will be reviewed annually as part of the policy review cycle.

Related Policies:

- Child Safety Policy
- Duty of Care Policy
- Internet Policy
- Student Engagement Policy
- Wellbeing and Discipline Policy