

Canterbury Public School Information Communication Technology (ICT) Acceptable Use Policy

Canterbury Public School is committed to embedding technologies within the curriculum in a way that is appropriate and acceptable in order to facilitate quality teaching and learning.

This Information Communication Technology and Internet Use Policy embeds the current DET Online Communication Services: Acceptable Usage for School Students Policy, the NSW DET Internet Use Policy, the CPS Anti-Bullying Policy and the Canterbury Public School Discipline Policy in order to ensure effective and appropriate learning environments when utilising ICTs.

This policy provides a consistent framework for ICT use in teaching and learning programs and strategies to manage inappropriate use of ICT.

Outline of policies embedded into the CPS Information and Communication Technology and Internet Use Policy

Online Communication Services: Acceptable Usage for School Students

1. Objectives - Policy statement

- 1.1 The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences with the NSW Department of Education and Training.
- 1.2 Use of the internet and online communication services provided by the NSW Department of Education and Training is intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.
- 1.3 Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.
- 1.4 Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.
- 1.5 Students who use the internet and online communication services provided by the NSW Department of Education and Training must abide by the Department's

conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6 Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

2. Audience and applicability

2.1 This policy applies to all school students located at NSW Government schools who access internet and online communication services within the NSW Department of Education and Training network and from any external location.

3. Context

3.1 This policy document takes account of the Memorandum Student Access to the Internet of 18 July 1997 and the Memorandum DN/04/00215 - Review by Schools of their Student Access to the Internet Policies.

3.2 This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.

NSW DET Internet Use Policy

- **Say No** - to using the computer to find, read or send anything rude, scary or unkind
- **Go** - to a responsible adult if you do and
- **Tell** - a responsible adult about anything that makes you feel uncomfortable

Canterbury Public School Discipline Policy

Everyone has the right:

- To RESPECT
- To be SAFE
- To Learn

Our School rules support this:

- I will show respect
- I will be safe
- I will learn

Canterbury Public School Anti-Bullying Policy

The school defines bullying behaviour, including cyber bullying, by a person or group that repeatedly makes another person or group feel that they are unsafe, uncomfortable or unhappy. The school recognises that bullying behaviour falls in to 4 categories; verbal, physical, social and psychological.

What is Information and Communication Technology (ICT)?

Information and Communication Technology (ICT) is an umbrella term that covers all technical means for processing and communicating information as well as well as techniques for storing and processing information.

For example:

- computer hardware
- computer software
- data Servers
- local area networks (LAN)
- internet

ICT is also used to describe digital technologies including methods for communication, transmission techniques, and communications equipment.

For example:

- the world wide web (Internet)
 - Web 2.0 (blogs and wikis)
 - Video Conferencing Equipment (Connected Classroom)
 - Email
- telecommunications
 - Mobile phones
 - SMS

The term has gained popularity partially due to the convergence of information technology (IT) and telecom technology.

ICTs include the following:

- computers
- hardware
- software
- digital cameras
- video cameras
- mobile phones
- scanners
- data projectors
- Interactive White Boards
- Internet
- data servers
- printers
- USB thumb drives



Expectations of ICT Use

Everyone is expected:

- to **respect** ICTs and use them appropriately
- **be safe** when using ICTs
- to access ICT and **use ICT for learning only.**

Our School rules support this:

- I will show respect
- I will be safe
- I will learn

Students will be aware that they will be held accountable for their actions and behaviour.

Students will not:

- damage computer equipment
- use ICTs for anything except learning
- let others use their email/learning account
- change computer settings
- interfere with school ICT systems (network, server)
- install any material (software, files, games) without permission from the Computer Coordinator
- download any material from the internet
- upload any material to the internet without permission
- ask (except the teacher) for or giving out any passwords
- publish information about teachers including email addresses
- access anything rude, scary or unkind.
- pass on anything rude, scary or unkind.
- send anything rude, scary or unkind.

Students will:

- tell a teacher if they get spam or a virus via email
- tell a teacher if someone they don't know, contacts them online
- be aware that all internet and online communication services can be traced
- keep their passwords a secret
- keep their personal details a secret (email, address, name, school, class...)
- ask permission to publish other peoples work
- ask permission from the Computer Coordinator/Principal to publish to the internet.

Expectations of ICT Use - Parent and Staff Version

Access and Security

Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal e-learning account.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
 - a message that was sent to them in confidence.
 - a computer virus or attachment that is capable of damaging recipients' computers.
 - chain letters and hoax emails.
 - spam, e.g. unsolicited advertising material.
- never send or publish:
 - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
 - sexually explicit or sexually suggestive material or correspondence.
 - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Training.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

Intellectual Property and Copyright

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.



Consequences for inappropriate use of ICTs.

The inappropriate behaviour will be assessed by the teacher, if necessary in consultation with the computer coordinator.

For minor misuse, such as:

- Lack of care when using ICTs (playfully throwing a camera around, hitting keyboard too hard...).
- Changing local computers settings.

Consequence - **verbal warning**, but if a particular student displays repeated behaviour (2 warnings and time out) a support desk slip should be filled out and the computer coordinator need be made aware.

For major misuse, such as:

- Logging on as another person.
- Using computers for anything other than school work.
- Using USB drives at school.

Consequence - **a support desk slip** should be filled out and the computer coordinator needs to be made aware.

1 slip = Loss of right to use ICT for **1 week** (parent's notified by the computer coordinator)

2 slips = Loss of right to use ICT for **2 week** (parent's notified by the computer coordinator)

3 slips = Loss of right to use ICT for **10 weeks** (parent's notified by the computer coordinator)

For serious misuse, such as:

- issues related to cyber bullying
- intentionally accessing inappropriate content
- recording content without prior permission from a teacher
- publishing content to the internet without prior permission from a teacher

Consequence - an **interview** will be arranged with student, parent/s, computer coordinator and principal. Consequence will be an automatic **lost of the right to use ICT for 10 weeks**.
