

St Pauls Catholic College

Student Acceptable Use of ICT Policy.

Both students and parents/guardians must read and sign this policy.

The purpose of Information and Communication Technologies (ICTs) at St Pauls Catholic College is to:

- Enhance student learning opportunities.
- Promote student achievement.
- Support the professional work of staff.
- Enhance the school's management information and business administration systems.

The use of these ICTs within school should be responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this policy. This policy applies to the use of all school related ICTs for educational purposes, whether provided by the school or the student.

Student information - Name, Class, and Email may be given to external providers engaged by the College. A copy of each provider Privacy statement is available on their website.

Definitions

Information and Communications Technologies are any electronic device or related applications which allow users to record, send, access, or receive information, in textual, audio, image or video form. These may include but are not restricted to:

- Computer systems and related applications such as email and Internet.
- Web-based tools such as discussion forums, chat rooms, blogs, pod casts, social networking sites and instant messaging systems.
- Mobile devices.
- Fax machines.
- Imaging tools such as video or still cameras.
- Audio tools such as audio recording devices.
- CeNet.

Acceptable uses

Students should:

1. Respect resources

- Use ICT equipment and resources for educational purposes under teacher supervision.
- Follow teacher directions for accessing files, programs, email and Internet resources.
- Seek advice from a teacher before responding to online prompts.
- Delete emails from unknown sources without opening any attachments as they may contain a virus.

2. Respect others

- Respect the rights, beliefs, and viewpoints of others.
- Follow the same standards of behaviour online as you are expected to follow in real life.
- Follow the Netiquette guidelines for online communications at the end of the document.
- Observe copyright rules by respecting the information, ideas and artistic works of others.
- Acknowledge the author or publisher of information from the Internet and do not claim the work or pictures as your own.

3. Keep yourself safe online

- Keep your passwords and personal work secure.

- Use the Internet and email for educational purposes only.
- Use school provided email accounts when communicating online.
- Seek teacher advice before providing personal details online.
- Always get teacher permission before publishing any personal information or photos online.

Unacceptable uses

The following uses of ICTs are considered unacceptable:

1. Personal safety

Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

You should **NOT**:

- Send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes home address, telephone or mobile number, school address, work address, email addresses, etc
- Meet with someone you have met online without your parents/guardian's approval and participation.

2. Illegal activities

Students need to be aware that they are subject to laws relating to assault, trafficking and computer offences.

An electronic audit trail may provide evidence of offences.

You should **NOT**:

- Attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails.
- Make deliberate attempts to disrupt other people's use of ICTs.
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
- Engage in any illegal act, such as threatening the personal safety of others, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, etc.
- Install or use software which is not licensed by the school.
- Install the College profile on more than one mobile device.

3. Network security

You should **NOT**:

- Provide your password to another person or in response to a request via email (even if it looks like the email comes from someone you know).
- Go looking for network security problems, because this may be seen as an attempt to gain unauthorised access to the network.
- Post information that, if acted upon, could cause damage to or disrupt the network.
- Open e-mails from unknown sources.
- Download any digital content without express permission of staff.
- Leave the computer while logged onto the network.

4. Inappropriate language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Messages sent using the school's ICTs may be monitored or scanned.

You should **NOT**:

- Use obscene, profane, rude, threatening, sexist, racist, disrespectful, or inappropriate language.

5. Respect for privacy

You should **NOT**:

- Re-post a message that was sent to you privately without the permission of the person who sent the message.
- Take photos, sound, or video recordings of people, including background figures and voices, without their permission.
- Distribute private information, including photos or recordings, about another person without their permission.
- Send or post any digital content relating to and or identifying the College or Staff without the express permission of the Principal.

6. Respect for others

You should **NOT**:

- Make personal attacks on another person.
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells you to stop sending them messages, you must comply with their request.
- Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people or organisations.
- Send or post personal information about other people without their permission.
- Send or post any digital content that may be found to be offensive by others.

7. Respecting resource limits

You should **NOT**:

- Use ICTs for other than educational activities and limited, high quality, self discovery activities.
- Download or send large files (>5 Mb) without Teacher permission.
- Post or respond to chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- Store any unauthorised material on the College network.

8. Plagiarism and copyright

You should **NOT**:

- Plagiarise works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Use material from the Internet in a manner which violates copyright laws.
- Access or use material from the Internet which relates to exam cheating or providing completed assignments.

9. Access to inappropriate material

Attempts to access inappropriate material using the school's ICTs is monitored and logged by the College or CEDP.

Some inappropriate material may be filtered or blocked by the College or CEDP.

You should **NOT**:

- Use ICTs to access material that:
 - is profane or obscene (pornography).
 - advocates illegal acts.
 - advocates violence or discrimination towards other people.
- Participate in online chats, discussion groups or mailing lists that are not relevant to your education.
- Access material which is not relevant to your education.
- Use the school ICTs to purchase, order or sell any goods.

A special exception may be made if the purpose of such access is to conduct educational research and both the teacher and the parent/guardian approve access.

Notification

You should:

- Disclose to your teacher any messages you receive that are inappropriate or disturb you.
- Notify the IT Dept of the College if you identify a possible security problem.
- Immediately disclose accidental access to inappropriate material to the IT Dept. of the College. This will protect you against an allegation that you have intentionally violated the Acceptable Use Policy.
- Notify the IT Dept. at the College if you are offended by another person's use of ICT.

Consequences of improper use

Any user violation will be recorded and may be subject to the following consequences:

- Loss of access privileges for a period of time.
- Dealt with in accordance with the College discipline policy according to the nature and severity of the breach.
- Informing parents/guardians.
- Legal action.

Netiquette

Netiquette refers to the guidelines and etiquette for online communication

You should:

- Ensure that email and online messages are written carefully and politely. You should also try to keep messages short and precise.
- Check e-mail frequently and delete unwanted messages promptly.
- Use appropriate language. Anything you post online is public.
- Be cautious in using humour and satire as they can easily be misinterpreted.
- Respect the rights, beliefs and viewpoints of others.
- Follow the same standards of behaviour online as you are expected to follow in real life.
- Ensure Caps Lock is off when typing text, as typing in all capitals is equivalent to online shouting.

.....