Parent Resources

Cybersmart

Developed by the Australian Communications and Media Authority, Cybersmart is part of the Australian Government's cybersafety program. It provides resources and advice to young people and parents on managing the internet safely.

Visit: www.cybersmart.gov.au/

SpamMatters

To make a complaint about spam email, IM, SMS and MMS messages:

Tel: 1300 855 180

Visit: www.acma.gov.au/spam

Or you can forward spam sent on mobile phones to the following number: 0429 999 888.

SCAMwatch

Recognise, report and protect yourself from scams.

Tel: 1300 302 502

Visit: www.scamwatch.gov.au

ThinkUKnow

ThinkUKnow is an internet safety program run by the Australian Federal Police and Microsoft and supported by ACMA.

Visit: www.thinkuknow.org.au

The Alannah and Madeline Foundation

The Alannah and Madeline Foundation's Cybersafety and Wellbeing Initiative aims to make cybersafety a normal part of every young person's life.

Visit: www.amf.org.au/cybersafety/#section2

Str8TLK

Str8TLK provides information on mobile phones for young people by the Australian Mobile Telecommunications Association.

Visit: www.str8tlk.amta.org.au

ChatDanger.com

ChatDanger.com provides advice about online and mobile chat and interactive services.

Visit: www.chatdanger.com

Stay Smart Online

Advice on smart online habits including shopping, socialising and banking.

Visit: www.staysmartonline.gov.au

FOR HELP & GUIDANCE

Kids Helpline

Telephone and online counselling for Australian children and young people.

Tel: 1800 55 1800

Visit: www.kidshelp.com.au

Reach Out

Information and support for young people to help them through tough times.

Visit: www.reachout.com.au

Email: info@reachout.com.au

Beyond Blue

Information for Australians about depression.

Visit: www.beyondblue.org.au

Life Line

Telephone counselling and online advice and support – 24 hours.

Tel: 13 11 14

Visit: www.lifeline.com.au

JOHN PAUL COLLEGE
WITH HIM IS THE FULLNESS OF LIFE

Cybersafety User Agreement

INTRODUCTION

Central to John Paul College's Mission is the importance of preparing students with the skills and values to engage successfully in the twenty first century world. This requires that students must proficiently navigate an increasingly sophisticated cyber world that will be central to their educational, professional and social lives. To do this the College is committed to providing them with learning that includes values such as mutual respect and personal responsibility, alongside skills in critical thinking and Information and Communication Technology (ICT).

This Cybersafety User Agreement outlines the expectations and responsibilities of all members of the John Paul College Community as it impacts upon ICT. It has been developed in the context of existing College policies and procedures including:

- Safe School Policy (formerly Anti-Bullying Policy)
- ICT Policy & Procedures
- Student Code of Conduct

School & Home Partnership - Shared Values & Shared Responsibility

Twenty first century students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

At John Paul College we believe the teaching of cybersafe and responsible online behaviour is essential in the lives of students and is best taught as a partnership between home and school. Safe and responsible behaviour is explicitly taught at our College and parents/carers are requested to reinforce this behaviour at home.

This User Agreement applies to all students during school and while on excursions, camps and co-curricular activities. We also recognise that inappropriate use of personal ICT out of school hours can have an impact upon the College community. John Paul College does not tolerate any form of bullying or harassment, personal attacks or defamation whether of students or staff at any time.

Therefore, this User Agreement encompasses the use of:

All JPC technology at school

ICT brings many benefits to the teaching and learning programs. While it is a valuable tool, it must be used responsibly. While our College has positive cybersafety practices in place, the nature of the internet means that full protection from inappropriate content can never be guaranteed.

Due to the various sources and locations of access to the internet, it is important to acknowledge that at times, students may have unsupervised access to the internet and email.

All personal technology used at school

While these devices (personal mobile communication and storage devices including mobile phones, blackberries, memory sticks, flash drives, ipods, mp3 layers, cameras etc) are privately owned, the guidelines outlined in this User Agreement also apply whenever these devices are used at school or on any school related event.

Mobile communication devices often have open access to the internet. However, the College has no control over the use or misuse of these devices and cannot filter or monitor usage or content.

Students need to be aware that content on personal devices brought to school or on any school related activity must be appropriate to the school environment.

Online behaviour outside of school impacting upon College Community members

This User Agreement outlines expected behaviour and possible consequences for any inappropriate on line behaviour which impacts upon students and staff at John Paul College. Students involved in the creation and dissemination in the public domain of any harassment or defamation of a member of the JPC Community (e.g. by SMS, online or social networking sites, blogs or emails) could face disciplinary action at school. Serious incidents may require the College to inform the police.

The overall goal of the College in all of these matters is to create and maintain a cybersafety culture which is in keeping with the Mission and Values of the College, and legislative and professional obligations.

CYBERSAFETY RESPONSIBILITIES

John Paul College will:

- Do its best to keep the College cybersafe. This includes working to restrict access to inappropriate, harmful or illegal material on the internet or College ICT equipment and devices.
- Make use of filtering and/or monitoring software to do our best to restrict access to certain sites and data.
- Do its best to provide supervision and direction in internet activities.
- have a school intranet which is accessed by school community members and is only
- Provide education about ethical and cybersafe behaviours including information about digital rights and privacy to compliment and support the User Agreement.
- Respond appropriately to any breaches of the User Agreement

Students are expected to:

- Observe College expectations as stated in the JPC Safe School Policy, ICT Policy and Procedures and the Student Code of Conduct (see Student Planner).
- Use equipment correctly to ensure that no damage occurs (This includes creation, introduction or spreading of viruses, physically abusing hardware, altering software settings, etc.)
- Refrain from accessing inappropriate information and/or sites on the internet.
- Allow priority use of the network to students who have school work to complete.
- Obey any restrictions on Internet, chat rooms, email or game use that may be applied from time to time;
- Not intentionally sending or displaying offensive messages or pictures. (If you wouldn't want your parents to see it, don't access it or write it.)
- Protect their personal details on the Internet;
- Ask their teacher's permission before using MP3 music players (e.g. iPods) in class.
- Comply with copyright laws (e.g.: plagiarism – copying web content without referencing it in their work) or publish libellous comments;
- Not post any defamatory or inappropriate comments or images on personal blogs, discussion forums or web sites.
- Show respect for others' privacy and their intellectual property;
- Report any misuse of our facilities to staff.

ICT Use At Home: Suggestions for Parents

At school the internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, it is increasingly being used as a social space to meet and chat. We encourage parents to make use of the rules outlined in this User Agreement as a basis for student use at home. John Paul College, however, cannot take responsibility for student ICT use at home. To support parents in managing ICT use at home we have included some further advice and recommendations below.

We recommend that parents:

- For students up to and including Year 10, put access to the internet in a public space in the home, including when using a wireless connection – not in bedrooms.
- Encourage your children to show you what they are doing on the internet. Find out how your child uses the internet and who else they connect with online. Discuss and encourage critical thinking skills.

Ask questions such as:

- How does it work and how do you set it up?
- Who is else is sharing this space or game - do you know them or did you 'meet' them online?
- Can you see any risks or dangers in the activity - what would you say to warn/inform a younger child who might come across this site?
- What are you doing to protect yourself or your friends from these potential dangers?
- When would you inform an adult about an incident that has happened online that concerns you? (Discuss why your child might keep it to themselves.)

Also

- Try to get to know your child's 'online friends' – just as you would try to get to know their other friends.
- Teach your children to never give out personal information whilst on the internet. Discuss with them what personal information actually is. It is likely that what you think is personal, they may not. Encourage them to never share pictures of themselves or the family with anyone they meet online.
- Set reasonable rules and guidelines for computer use and discuss these with your children. Monitor the amount of time your children spend online. Real life interactions need to balance online time.
- Use a separate log-in for each member of the family. Regularly check where your children have visited on the internet.
- Talk to parents of your child's friends about their rules for cybersafety.
- Teach your child protective behaviours and safety procedures related to the cyber world as you would for other parts of their lives. They need to feel comfortable coming to you with concerns.
- Avoid punitive responses such as indefinite banning of things to do with ICT use. This is likely to lead to resentment and secrecy.
- Get to know the internet safety sites and check them regularly for safety advice. Use appropriate filtering software, and keep your computer secure. Regularly update anti-virus, anti-spyware, spam filters and firewalls.
- Teach your child cyber ethics. For example, hacking into someone's computer is just as wrong as breaking into a house.