Immaculate Heart of Mary School

2023 CYBER-SAFETY AT IMMACULATE HEART OF MARY SCHOOL

Dear Parents and Caregivers,

At Immaculate Heart of Mary School there are many opportunities for students to use Information and Communication Technologies to further develop their learning. We have a network across the school and students have access to information through a variety of means – from iPads, laptops to information stored on the School Network as well as the Internet.

The measures to promote cyber-safety at IHM are based on our pillars of Love, Hope, Justice, Connectedness and Inclusivity. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we require you to read this document, discuss with your child and sign the attached Use Agreement Form.

Rigorous cyber-safety practices are in place, which include cyber-safety 'Use Agreements' for staff and students. Child protection education, such as the Keeping Safe Child Protection Curriculum and our school based social and emotional learning program, include information about keeping safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Immaculate Heart of Mary, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to our school, whether it is used on or off the site.

The overall goal of Immaculate Heart of Mary is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The 'Use Agreement' includes information about your obligations, responsibilities and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students will be issued with a 'Use Agreement' and once signed consent has been returned to school, students will be able to use the school ICT equipment. Material sent and received using the school network may be monitored and filtering and/or monitoring software is used to restrict access to unsuitable sites and data, including e-mail.

We recommend the use of appropriate filtering software at home. Please note that IHM does not recommend for children to be part of a social network if they are 13 years of age or under. Information about Internet filtering can be found on the websites of the **Australian Communications and Media Authority** at http://www.acma.gov.au, **NetAlert** at http://www.netalert.gov.au, the **Kids Helpline** at http://www.kidshelp.com.au and **Bullying No Way** at http://www.bullyingnoway.com.au

Please do not hesitate to contact me if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Kind regards,

A Diassinas

Annette Diassinas
ACTING PRINCIPAL

STRATEGIES TO HELP KEEP IHM STUDENTS CYBER-SAFE

Important Terms

'Cyber-safety' *refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.*

'Cyber bullying' *is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.*

'School *ICT*' *refers to the school's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.*

'ICT equipment/*devices*' *includes computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, iPads, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), wearable technology (e.g. smart watches) and any other, similar technologies.*

'Inappropriate material' *means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment.*

'E-crime' *occurs when computers or other electronic communication equipment/devices (e.g. Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.*

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies, to help them stay safe when using ICT at school and after formal school hours.

1. I will not use school ICT equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to school. The school cyber-safety strategies apply to any ICTs brought to school.
2. I will use the computers and other ICT equipment only for my learning and teacher directed activities.
3. I will not access social networking or gaming sites at school or download any games or music etc onto the school network.
4. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
5. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.
6. I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.
7. I will keep my password private.
8. I will not store personal files, including music, games or pictures, on the School Network.
9. I will use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
10. **While at school, I will:**
    - attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing.
    - report any attempt to get around, or bypass security, monitoring and filtering that is in place at our school.
11. **If I find anything that, is mean, rude, unacceptable or upsets me, I will:**
    - not show others
    - turn off the screen
    - notify a teacher straight away.

Only with written permission from home and the school will I bring any ICT equipment/devices to school. This includes things like mobile phones, wearable technology (e.g. smart watches) and any other, similar technologies, iPods, games, cameras, and USB/portable drives.

12. If a mobile phone, smart watch or iPad needs to be brought to school this must be handed into the office in the morning and collected at the end of the school day.

13. To ensure my compliance with copyright laws, if I download or copy any files such as music, images, videos, games, or programs I will acknowledge the owner.

14. I will not put any personal information online, unless a parent or teacher has given permission. Personal identifying information includes any of the following:

- my full name
- my address
- my e-mail address
- my phone numbers
- photos of me and/or people close to me.

15. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:

- not intentionally disrupting the smooth running of any school ICT systems
- not attempting to hack or gain unauthorised access to any system or network
- following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
- reporting any breakages/damage or inappropriate use to a staff member.

16. If I do not follow cyber-safety practices the school may inform my parents/caregivers and my access to any ICT's at school may be suspended.

In serious cases, the school may take additional disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

CYBER SAFETY, SOCIAL MEDIA AND YOUR CHILD

As a school, we do all we can to educate children and parents about the importance and necessity of cyber safety. It is part of our curriculum and all measures are put into place in the school to ensure blockage of inappropriate sites and content, as well as promoting responsible and safe use of the internet.

We remind all parents that Social media services like Facebook, Twitter, Instagram, Pinterest and Snapchat **require account holders to be at least 13 years old in accordance with the** Children's Online Privacy Protection Act (COPPA).

Monitoring your child's online behaviour at home is a **parental responsibility** and the easiest way to do this is to abide by the social media age limits and not succumb to the "but everyone is on it!" argument.

As a parent it is important that you are fully aware of how your child uses the internet and social media, particularly out of school hours. There are inherent dangers of children under the age of 13 having social media accounts as this makes children susceptible to cyber predators, cyber bullying and other potentially very dangerous situations.

In addition, 13 is the general developmental age when children start developing a broader understanding of the world around them and along with that a **better sense of what's appropriate to share on line.** As young teens, children are also developing a desire to control more of their activities as well as **the maturity to handle that control.**

As a school, **we seek your support in ensuring your child is acting appropriately and safely** if and when using social media or the internet out of school hours. This will help to ensure that issues and problems that can spill into school life, and waste important learning time at school, do not arise.

We can and do take the time to talk to the children, to encourage their responsible and safe use of social media. We also report known misuse to parents immediately, as **the ultimate responsibility and control is yours.**

If your child does end up joining a social network, despite this advice, here are some ground rules that have been recommended by authorities on cyber safety that work for many parents:

Use privacy settings:
Privacy settings aren't foolproof, but they can be helpful. Take the time to learn how privacy settings work on your kids' favourite sites and apps, and teach your kids how to control the information they make public or private. Encourage them to check privacy settings regularly, since sites' policies often change. Tell your kids to think before they post. Remind them that everything can be seen by a vast, invisible audience (otherwise known as friends-of-friends-of-friends), and, once something's online, it's hard to take back.

Be a friend and follower:
Each family will have different rules, but, especially for younger kids, it's a good idea for parents to have access to their kids' pages, at least at first, to be sure that what's being posted is appropriate. Parents can help keep their children from doing something they'll regret later.

Keep private information private: Don't share your home address or other sensitive information online.

Be respectful of others:
Kids may use social media to act out because they feel anonymous and that their actions are consequence-free. Make sure they understand that the Internet is a giant community that works best when everyone respects each other.

Report any misuse: to the social networking site so that inappropriate usage is blocked.

I trust that this information and advice is of use to you in setting appropriate boundaries and talking with your child about the safe and responsible use of social media.

More information can be found on our school website, on social media sites under conditions of use, and at this esafety government website: https://www.esafety.gov.au/education-resources/iparent

2023 CYBER-SAFETY USE AGREEMENT FORM

To the Parent/Caregiver / Legal Guardian:

Please read this page carefully to check that you understand your responsibilities under this agreement, **sign the Cyber Safety Use Agreement attached and return to the school.**

I understand that Immaculate Heart of Mary will:

- do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on ICT equipment/devices at school or at school-related activities
- work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the Use Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate manner
- welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

My responsibilities include:

- discussing the information about cyber-safety with my child and explaining why it is important
- supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
- contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or this Use Agreement.

PLEASE RETURN THIS SECTION TO SCHOOL

2023 CYBER-SAFETY USE AGREEMENT

We have read, discussed and understood this Cyber-safety Use Agreement and are aware of the school's initiatives to maintain a cyber-safe learning environment and also of IHM's position on social media.

Name of Child..... **Class** .....

Signature.....

Name of Parent/Caregiver/Legal Guardian.....

Signature..... **Date**.....