Cybersafety, Internet and School ICT Usage Policy

Important terms used in this document:
(a) The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
(b) '**Cybersafety**' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.
(c) '**School ICT**' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below.
(d) The term '**ICT tools/equipment/devices**' used in this document, includes but is not limited to, computers (such as desktops, laptops, iPads), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile/smart phones, video and audio players/receivers (such as portable CD and DVD players), and any other technologies as they come into use.

Rationale:
Holy Spirit strives to create a supportive learning environment where students feel safe and secure and in which a sense of belonging and wellbeing is strengthened (Holy Spirit Wellbeing Policy). Contemporary learning environments include the use of ICT resources, as well as networked and internet based resources and communities. Holy Spirit School has a responsibility to ensure the physical and emotional safety and wellbeing of students and staff engaging in these environments.

Holy Spirit School acknowledges the benefits of ICT and the Internet and their relevance to all learning strands. We recognise the central place of technology in the current and future worlds of our students and their need to be able to access these technologies, including online technologies and communication. Our learners need to develop the skills and knowledge necessary to learn about and to participate as active citizens in an ever-changing world. Holy Spirit School acknowledges that, with access to online and networked resources, comes the need for opportunities for students to learn about safety, moral and ethical issues associated with their use. Holy Spirit has the dual responsibility to maximise the benefits of these resources, whilst at the same time minimise and manage the risks.

Holy Spirit thus acknowledges the need to have in place explicit and effective cybersafety practices which are directed and guided by this policy.

This policy directly relates to the requirements of the Child Safe Standards.

Aims of Policy:
- To adopt a harm minimisation approach to the safety of students working with School ICT tools
- To align cybersafety practices with the school's Student Wellbeing Policy
- To guide the development of explicit strategies to target the cybersafety knowledge and skills of students Prep-6
- To ensure that all staff are confident, skilled, supported and proactive in relation to cybersafety issues
- To develop protocols that are clear and well understood by the school community, to ensure the effectiveness of school cybersafety and security practices
- To provide digital learning environments that value and build positive social and learning behaviours
- To promote the use of ICT devices at school and at home
- To build positive home-school partnerships in relation to ICT use and cybersafety issues

Elements of this Policy:
This policy will address these points:
1. POLICY GUIDELINES
2. USER AGREEMENTS
3. MONITORING USE
4. AUDITS
5. WORKING ONLINE
6. APPROPRIATE USE AND ACCESS and SCHOOL ICT USER PROTOCOL
7. BREACHES
8. OTHER ASPECTS OF SCHOOL CYBERSAFETY
9. STUDENT SCHOOL ICT USER AND CYBERSAFETY AGREEMENT

Appendices:

A – Working Online Policy
B – Tips for Bridging the Gap

Guidelines for Implementation:

- Our school actively supports access by students to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret and evaluate information encountered.
- All staff and students will have internet and email access (staff and Years 2-6 students). Such access is a privilege that infers responsibility, and not simply a right to be expected.
- Use of the computer network and internet and the cybersafety of students are overseen by the Principal and e-Learning Leader.
- The management of the school network and school ICT devices/equipment is undertaken by a designated technician and overseen by the principal and e-Learning leader.
- The school undertakes to ensure that information published on the Internet by students or the school is of a high standard, and meets legal requirements and standards of general practice within the community in relation to copyright, safety and decency.
- All user accounts will be password protected and users will be responsible for maintaining user accounts, including clearing content regularly.
- All staff members are responsible for maximising the safety of students when working with ICT and in networked and online environments.
- Students' development in the area of ICT is planned for using an integrated approach and reported on using national and statewide standards.
- The staff are familiar with the Internet and Network Usage policy, clearly communicate agreed behavioural expectations and respond appropriately and consistently to student behaviour in online learning environments
- Holy Spirit implements strategies related to cybersafety
- Staff members provide a safe school environment and are aware of their legal obligations to perform their duty of care to students
- The school works with all members of the school community, including families, to promote, educate and enhance the safe and responsible use of technology
- The staff participates in regular staff meetings, professional development and will liaise with community organisations in order to ensure that they are confident, skilled and proactive in relation to e-Learning, student wellbeing and safety issues.
- Privacy of students, parents, staff and other users must be recognised and respected at all times.
- Users are responsible for notifying teachers and appropriate leadership staff of any access issues, including issues related to passwords and inappropriate material.
- Signed parent consent and a user agreement signed by users (students and staff) is required to be completed in order to gain access to the internet, or to publish work, photos or videos on the internet.

Evaluation:

The Cybersafety, Internet and Network Usage Policy will be evaluated and reviewed as part of the 4 year School Review cycle.

Cybersafety, Internet and School ICT Usage Policy

1). POLICY GUIDELINES

1.1 This internet and network usage policy will cover all employees, all students and any other individuals granted permission to use and access School ICT.

1.2 The use of Holy Spirit's computer network, Internet access facilities, computers and other ICT equipment/devices is limited to educational, administrative and creative purposes appropriate to the school environment.

1.3 Students are provided with time to use ICT resources for a variety of activities that promote learning across all learning domains. One aspect of this learning involves the use of the email and the Internet as a source of information and a means of communication.

1.4 Holy Spirit Primary School, Thornbury East provides the opportunity for both email and Internet access to relevant and current information on the World Wide Web. All email and Internet access at Holy Spirit is via our Local Area Network (LAN) and the Catholic Education Network Victoria and is filtered via the CEVN.

1.5 The use of privately-owned ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. Equipment/devices could include a mobile phone, camera, recording device, or portable storage (such as USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the Principal and/or school leaders.

1.6 Students' development in the area of ICT is reported on using the national and statewide standards.

2). USER AGREEMENTS

2.1 All staff and students will be issued with a user agreement. Parents are required to read these pages carefully, discuss them with their children, and return the signed agreement to the school office for filing. Students from Years 2 – 6 are required to read, discuss and sign this agreement. Staff are required to read and sign a user agreement. All agreements will be filed and stored.

3). MONITORING USE

3.1 Holy Spirit has the right to monitor, access, and review all electronic work and communication and ICT devices. This includes personal emails sent and received on the school's computers and/or network facilities, and search terms used either during or outside school hours if a need arises.

3.2 Within the Catholic Education network web search terms and email content are monitored and reported on. Access to certain sites such as social networking and some web based email is restricted within this network.

3.3 The school may request permission to audit privately-owned ICT equipment/device(s) where a suspected breach of the internet and network usage policy has occurred.

3.4 Users must not attempt to circumvent monitoring or filtering.

4). AUDITS

4.1 The school will occasionally conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, may commission an independent audit, or be audited by the Catholic Education Melbourne.

4.2 Where deemed necessary stored content will be deleted. Staff and students will be notified prior to this taking place.

5). APPROPRIATE USE AND ACCESS

5.1 All teachers and students using these facilities are required to do so in an appropriate, safe and responsible manner. Failure to do so will be considered a breach of the user agreement. Student access to email and online resources must be under teacher direction of the highest standard possible.

5.2 The use of personal devices, including but not limited to mobile phones, smart phones, iPods and iPads, at school by students is prohibited without the explicit permission of staff. Personal devices should not be brought to school without permission from staff and must remain switched off and out of sight, unless being used for explicit learning purposes.

5.3 Catholic Schools are connected to a private network with the Catholic Education Melbourne and users access the internet within a filtered cache. These measures help filter out inappropriate sites and material however, it may not always be possible for the school to filter or screen all material. This may include material which is inappropriate in the school environment.

5.4 All users are to abide by the following **School ICT User Protocol** that has been developed for the school. This policy is to be viewed in conjunction with the *Student ICT User and Cybersafety Agreement* and the accompanying information for parents.

SCHOOL ICT USER PROTOCOL

1. Students will use the Internet and School ICT only with teacher permission and under teacher supervision.
2. Teachers are to assume responsibility for the email and Internet use of children in their care, both in formal class and out of class time (such as wet-day programs).
3. Internet sites searched and accessed should generally fit with the overall class program. Teachers are free to give either general or specific advice to students, depending on the work at hand.
4. Should browsing be allowed in non-class times, the same procedures apply but the students have more freedom in choosing the parameters of the sites that are searched and visited.
5. Access to interactive resources, such as forums, blogs and collaborative documents, is to be strictly supervised by teachers.
6. Access through the Catholic Education Network, Victoria is subject to filtering through Zscaler. However, should users come across sites or information that they feel is questionable they should:
   - *not proceed any further*
   - *use the "Back" button on their browser or close the window immediately*
   - *notify their teacher straight away*

7. Students and teachers will not provide identifying data, such as full name, address or other information that describes the personal situation or location of students, staff or community members
8. Students and teachers will be made aware of legal and ethical implications of inappropriate behavior, such as emailing or posting abusive, obscene or harassing messages, or using the school systems for unauthorised activities.
9. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorised access to the system.
10. Random checks of email, search terms and visited web sites will be part of the supervision process of the ICT lead teacher; or as requested by the School Principal.
11. Users will not download or install unauthorised programs onto School ICT devices.
12. Users will operate within copyright restrictions.
13. Users must not attempt to circumvent monitoring or filtering.

6). BREACHES

Breaches of the network user protocol can undermine the values of the school and the safety of the learning environment.

6.1 The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors on a case by case situation. Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action in line with the school's positive behaviour policies.

6.2 If there is a suspected breach of use agreement involving privately-owned ICT e.g. (smart phone, iPod) on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

6.3 Unsafe, mean, bullying or harassing behaviour online that involves community members targeting another community member may be investigated by the school. Behaviour that involves students may be managed according to this policy.

6.4 Involvement with material which is deemed inappropriate in a school setting, is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as cyber bullying. In such situations parents will be contacted and it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.

7). OTHER ASPECTS OF SCHOOL CYBERSAFETY

7.1 Students will be explicitly taught skills and behaviours appropriate to their developmental level to promote safe online behaviours and to help students to be cybersafe in all areas of their lives.

ALL FAMILIES TO SIGN

STUDENT NAME: ______________________________________ **CLASS:** _________

STUDENT SCHOOL ICT USER AND CYBERSAFETY AGREEMENT 2016-17

When I use the school computers and Internet, I have responsibilities and rules to follow.

I WILL:

- keep myself and my friends safe by not giving out personal details including full names, telephone numbers, addresses and images
- protect my passwords
- be respectful in how I talk to and work with others online
- use the technology at school for learning
- use the equipment properly and not knowingly damage hardware or content/programs contained on devices
- remember that the content on the web is someone's property and ask my teacher to help me get permission if I want to use information or pictures
- think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me or answer any questions (I should not copy and paste the information as my answer).
- talk to my teacher or another adult if:
  - I need help online
  - I am not sure what I should be doing on the Internet
  - I come across sites which are not suitable for our school
  - someone writes something I don't like, or makes me and my friends feel uncomfortable or asks me to provide information that I know is private.
  - I feel that the safety of other students at the school is being threatened by online activities

- should I come across sites or information that I feel are unsuitable, I will:
  - not go any further
  - use the "Back" button on my browser or close the window immediately
  - notify my teacher straight away

I WILL NOT:

- write mean, rude or offensive things about anyone
- participate in online (cyber) bullying
- bring or download unauthorised programs, including games, to the school or run them on school devices
- interfere with the work or data of another student, including on shared documents
- go looking for rude or offensive sites
- not ask anyone about their passwords, get, use or change the passwords of others
- not copy, change, use or delete files belonging to others
- access personal social media sites at school

I UNDERSTAND THAT:

- my email, files and internet search terms will be checked by teachers
- other ICT equipment/devices belonging to me, such as USB drives or mobile phones, may be checked by teachers
- the consequences for doing the wrong thing when using the computers or the Internet are the removal of my computer/Internet privileges. Serious misbehaviour will result in more serious consequences.

I acknowledge and agree to follow these rules. I understand that I may not be able to access the computers at school if I do not act responsibly.

⇨ Student Signature: ____ (students in Years 2 – 6)

Parent Permission (all parents to sign)
I agree to allow my child to use the Internet at school. I have discussed the scenarios, potential problems and responsible use of the Internet with him/her as outlined in the agreement and accompanying letter.
I will contact the school if there is anything here that I do not understand. If there is a situation which concerns me, I will contact the school.

⇨ Parent/Guardian Signature: ___________________________________ Date: _____________________

YEAR 2 – 6 FAMILIES ONLY

Online Tools and Learning Environments Permission

Holy Spirit School utilises various online tools and learning environments for learning and teaching in line with best contemporary practice. The use of online tools and environments is currently informed by the school's *Working Online Policy* and falls under our current ICT user agreement. The use of online tools carries with it the same responsibilities of all other computer and internet use including, but not limited to: the protection of personal information including log in details, the use of appropriate language, and the use of the tools for school-related purposes.

Students in Years 2-6 also use digital platforms as an online portfolio of their work and learning. These blogs/platforms can only be accessed using a unique login and/or password.

The Google terms of use and Catholic Education Office Melbourne (CEOM) require explicit parental permission for Google account holders under 13. In giving permission parents/carers should be informed of the following:

Holy Spirit Primary School will provide document creation and online storage for learning through the Google Apps for Education service. Google has a network of system servers and back-up mechanisms that operate from various international locations and consequently account details and data may be transferred, stored and processed outside of Australia. In using the school's ICT systems users consent to this transfer, processing and storage of that information. In order to provide this service, the following data is required to be stored on Google's servers and includes student login information (First Name, Last Name, User name), and their network login password. The school has received advice that there is an agreement with Google to ensure privacy policies and security measures regarding the protection of personal information are in place. School staff members have the ability to access, monitor, use or disclose information and work created online for the purposes of administering the system and ensuring its proper use.

⇨ **I give permission for my child ____ to access**

(student name)

online tools and learning environments, including Google Apps for Education (GAFE) and online portfolios (blogs/Seesaw) using their own account.

_______________________________ _________________________ _________________

(parent name) ***(parent signature)*** ***(date)***

⇨ **I give permission for my child's image (photograph/video) to appear on their blog/Seesaw:**

Yes / No

_______________________________ _________________________ _________________

(parent name) ***(parent signature)*** ***(date)***

Appendix A

Working Online Policy

Rationale

‘Working online’ refers to the production and storage of data online. Typically, work stored in online environments may be accessed by multiple parties. Online environments (including Web 2.0 tools) allow members of the school community to collaborate, produce, consume and respond to ideas and information in a myriad of ways. Working in online environments allows students and teachers to collaborate, have equity of access to information, to produce text for authentic audiences and purposes, and develop flexible skills and ways of working pertinent to active citizenship in the twenty-first century.

Aims

- To improve student learning outcomes by increasing access to worldwide information.
- To enable students and teachers to work collaboratively in online environments and extend their repertoire of skills when using ICT tools
- To provide authentic contexts for practising safe online behaviours

Implementation

- The school’s ICT Policy and Internet Usage policy form part of the implementation and procedures for working online.
- Work produced or stored online by teachers and students should have restricted access to approved audiences/collaborators and be protected by password access or be accessible by ‘author invitation’ only.
- Explicit permission needs to be obtained from parents/guardians for students to work in online environments. This permission forms part of the ICT User agreement and permissions.
- Students’ use of online environments and their posting of content is directed and overseen by a teacher.
- Personal information, such as full names, addresses, phone numbers and email accounts, should not be stored online.
- Photos and other media content can only be included with parental/guardian permission.
- Staff should take reasonable steps to limit student identifiers (such as full names) in work that is stored online.
- Work and images submitted by students for inclusion online to public audiences need to be moderated by an adult.
- Editing of work online will only be undertaken by the author or a staff member.
- Authors need to be mindful of copyright laws and attribute sources of information, images and content that are not original.
- Comments about student work online will be moderated by a staff member.
- Comments must be phrased in positive language and bullying or comments of a negative nature must not be used.
- Students’ use of online environments and knowledge of appropriate and safe online behaviour will be supported by an explicit cyber-safety strategy.
- Agreed to ‘Terms of Use’ must be published on school blog and websites.
- These implementation guidelines must be adhered to when undertaking all work online related to school, whether working onsite at school or offsite.
- Users’ access to the internet and blog/websites may be restricted if they do not follow the implementation guidelines as set out above (as per the Internet Usage Policy).

Date of last review: June 2016 Date for Review: 2018

Appendix B

Tips For Parents: Bridging the gap between home and school

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, but it is increasingly being used as a social space to meet, play and chat. The Internet can be lots of fun.

If you have the Internet at home, encourage your child to show you what they are doing online. If not, see if you can make a time to visit the school to see their work.

At home we recommend you:

- make some time to sit with your child to find out how they are using the Internet and who else is involved in any online activities
- have the computer with Internet access in a shared place in the house – not your child's bedroom
- ask questions when your child shows you what they are doing, such as:
  - *how does it work and how do you set it up?*
  - *who is else is sharing this space or game - did you know them before or "meet" them online?*
  - *why is this so enjoyable – what makes it fun?*
  - *can you see any risks or dangers in the activity - what would you say to warn/inform a younger child?*
  - *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.*

Statistics show that students will not approach an adult for help because:

- they might get the blame for any incident
- they don't think adults "get" their online stuff – it is for students only
- they might put at risk their own access to technology by either:
  - admitting to a mistake or
  - highlighting a situation that might lead a parent to ban their access.

What has your child agreed to and why?

Not giving out personal details or details of other students including full names, telephone numbers, addresses and images and protecting password details.

Students can be approached, groomed, and bullied online. They also love to publish information about themselves and their friends in spaces like Instagram, Facebook, blogs etc.
We recommend they:

- don't use their own name, but develop an online name and use avatars.
- don't share personal details including images of themselves or their friends online
- password protect any spaces or accounts they have and protect that password.
- don't allow anyone they don't know to join their chat or collaborative space.
- are reminded that any image or comment they put on the Internet is now public (anyone can see, change or use it)

Being respectful online and not participating in online bullying

The online environment sometimes feels different. The language is different. Sometimes students say things online that they would never say to someone's face.

- being online can make students feel that they are anonymous
- the space or chat they use in leisure time might have explicit language and they will feel they have to be part of it
- often the online environment has very few adults.

Using the technology at school for learning, using the equipment properly and not interfering with the work or data of another student.

By just taking care with the equipment, printing and downloading from the Internet students can save time, money and the environment. Students often see the Internet as "free". Just looking at a page on the Internet is a download and is charged somewhere.

Not bringing or downloading unauthorised programs, including games, to the school or run them on school computers

The school connects all of the computers through a network. The introduction of unknown games or files could introduce viruses etc and these put all of the schools equipment and student work at risk.

Not go looking for rude or offensive sites.

Filters block a lot of inappropriate content but it is not foolproof. For students who deliberately seek out inappropriate content or use technology that bypasses filters, parents will be immediately informed and the student's Internet access will be reviewed.

Using the Internet at school to learn.

It is important to realise that there is a time for fun and a time for work (even on the Internet). Staying on task on the internet will reduce risk of inappropriate access and teach students strategies to use the Internet for their learning.

Remembering the content on the web as someone else's property and asking teacher to help get permission before using information or pictures

All music, information, images and games on the Internet are owned by someone. A term called copyright is a legal one and has laws to enforce it.
By downloading a freebee you can risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts. Remember if an offer is too good to be true, the chances are it is!

Thinking carefully about what is on the Internet, questioning if it is from a reliable source and using the information to help answer questions.

Not everything on the Internet is true, accurate or unbiased.
The school is teaching information literacy skills, which enables students to locate, evaluate, and use information effectively on the Internet.
Copying and pasting information can help organise arguments, ideas, and information but it is important that your child uses their own thoughts and language to express what they have learnt. If helping with homework ask open-ended questions. For example, saying to a student "Tell me about wombats" might encourage him/her to copy and paste facts about the wombat, but asking the question "What would a day in the life of a wombat be like?" encourages the student to think about different aspects of the animals life and draw together the different pieces of information they might have discovered.

Talk to my teacher or another adult if:
- I need help online
- I am not sure what I should be doing on the Internet
- I come across sites which are not suitable for our school
- someone writes something I don't like, or makes me and my friends feel uncomfortable or asks me to provide information that I know is private.
- I feel that the welfare of other students at the school is being threatened by online activities

The Internet has some really flashy and tricky ways to lead people into websites they never meant to visit. It is easy for us all to get distracted. We want students to ask for help in locating the information they need, and clarifying the task they have been set. Unfocused clicking through websites can lead to inappropriate content.

We also want the whole school community to keep their Internet environment as safe as possible so we ask that if your child sees a site they think should be blocked, to turn off their screen and let a teacher know.

Open communication between parents, teachers and students is the best way to keep students safe. Students will often share concerns with each other online. It is important that they tell a teacher and or parent when they are feeling uncomfortable or threatened online.
If you have any concerns about this agreement or Internet Safety in general contact either the school or the contact below

NetAlert is Australia's Internet safety advisory body for internet safety issues/ concerns contact them on 1800 880 176 or visit http://www.netalert.gov.au/
A free parent's handbook is available at http://www.netalert.gov.au/advice.html