SOPHIA MUNDI

Steiner Education and IB World School

# Online Communication, Mobile Phone, Interactive & Digital Technologies

## Procedures

Version 4.0

# 1 Policy

This policy is based on the principles of mutual responsibility and respect of all parties involved in the use of mobile phones. It requires accountability on the part of the user for his or her actions. It is designed to assist in managing the safe and responsible use of mobile phones by students and involves parents as partners in assisting their children in the proper use of mobile phones.

Students need to be protected from exposure to inappropriate online material or activities, to be aware of the risks associated with some online activities, and to adopt protective online behaviour. Sophia Mundi Steiner School makes every reasonable effort to achieve this by educating and informing students and parents, as well as by putting measures in place to monitor email traffic and internet access. All activities conducted using the school's interactive & digital technologies and /or the school's online services may be logged and accessed for administrative, legal or security purposes.

This policy has been developed to assist teachers to put in place school-based processes and procedures that will both protect and inform students and parents in their use of the school's online services.

# 2 Purpose and Background

Digital technology is part of our everyday lives. We recognise that the rapid advances in technology will continue to develop and create new opportunities and challenges.

The purpose of this policy statement is to promote appropriate and ethical use of online communication, mobile phones and interactive & digital technologies in a way that provides access to its benefits. This policy statement enables us to make decisions about online communication, mobile phones, interactive & digital technologies use, to assist us to be self-disciplined and 'in-control', and to form positive, personal relationships. These will ultimately improve our learning experiences.

The classroom, and other learning spaces are places for creativity, innovation, risk taking and critical thinking. Used poorly, online communication, mobile phones, interactive & digital technologies can create distractions from being active learners and can have a negative effect on learning focus and outcomes.

At Sophia Mundi, it is our responsibility to model and monitor best use of online communication, mobile phones, interactive & digital technologies. The way in which students can be assisted to take responsibility includes the assurance that consequences will apply for poor decision-making. Student decisions about use of online communication, mobile phones, and interactive & digital technologies that breach school expectations will result in a consequential approach, so that better decisions are made in the future.

# 3 Scope

This policy applies to the Principal, teachers and supervisors of students and students accessing online communication and/or services, mobile phones, interactive & digital technologies from any of the school's locations including, but not limited to, the school.

The policy also applies to students during School excursions, camps and extra-curricular activities.

# 4 Definitions

4.1 *Inappropriate Content*

Content that is considered unsuitable or harmful to students. It includes material that is pornographic, that promotes illegal activities, violence or prejudice on the grounds of race, religion, gender or sexual orientation.

4.2 *Online Services*

Any services including, but not limited to, email, calendaring, instant messaging, web conferencing, discussion groups, internet access, social media, Apps and web browsing, that may be accessed using the computer networks and services of Sophia Mundi Steiner School.

4.3 *Parent*

Includes guardians and carers and refers to a person who at law has a responsibility for the care, welfare and development of a student.

4.4 *Spam*

A generic term used to describe electronic 'junk mail.' That is, unwanted messages sent to an email account or mobile phone. Messages do not have to be sent out in bulk to be considered spam - under Australian law, a single electronic message can also be considered spam.

4.5 *Personal safety and security*

Sophia Mundi Steiner School accepts that parents may give their children mobile phones to protect them from perceived everyday risks involving personal security and safety. There may also be concerns about children travelling alone on public transport or commuting long distances to School. It is acknowledged that providing a child with a mobile phone may give some parents reassurance that they can contact their child – and vice versa- if they need to speak to them urgently before or after School.

4.6 *Responsibility*

It is the responsibility of students who bring mobile phones to School to abide by the guidelines outlined in this Policy. The decision to provide a mobile phone to their children should be made by parents/ guardians and parents/ guardians should be aware if their child takes a mobile phone to School. Permission to have a mobile phone at School while under the School's supervision is contingent on parent/ guardian permission in the form of a signed copy of the mobile phone usage agreement (Appendix A). Parents/ guardians and/ or the School may revoke approval at any time.

4.7 *Cyberbullying*

Cyberbullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. See Appendix D

# 5 Procedures and activities

## 5.1 General guidelines

- Online communication (through laptop, email, social media, SMS etc) must be done in a way that is ethical, lawful and respectful.
- Students must never photograph or record any person without their permission.
- Distribution, by forwarding, posting or sharing, of another person's images, video and/or personal information must not occur without their permission.
- Mobile hotspots (e.g. through any devices) are not to be used during the school day and school events.
- Proxies, VPNs, or other encrypted connections to the internet are not to be used at school.
- Unlawful activity or behaviour will need to be referred by the school to the appropriate authorities.
- It is a criminal offence to use a mobile phone or other devices to menace, harass or offend another person. It is not a matter of the intention of the perpetrator, but the perception of the recipient as to whether something is menacing, harassing or offensive.
- If restorative action undertaken by the school is deemed ineffective, the Principal may consider it appropriate to involve Victoria Police.

## 4.2 Mobile phones and smart devices

Mobile phones carried by students should be switched off and left at the mobile phone drop-in at the School office whilst under the School's supervision, before, during and after School hours.

Smart devices (e.g. smart watches, Fit bits, other wearable technology) are not permitted.

The school must receive a signed permission for student to have an online service account (Appendix A) and a signed acceptable usage agreement for secondary students (Appendix B) before granting students access to online services.

### *5.1.1 Mobile phone - Guidelines for exceptions*

- Exceptions to the above may be permitted only in very particular circumstances if the parent/guardian specifically requests it in writing for a specific period of time and the School approves it. Such requests will be handled on a case- by-case basis and should be directed to the Principal. Parents are reminded that in cases of emergency, the School office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.
- Students who have permission to have phones while on School premises before or after School, should use soundless features such as text messaging, answering services, call diversion and vibration alert to receive important calls.
- Mobile phones should not be used in any manner or place that is disruptive to the normal routine of the School.
- Students should protect their phone numbers by only giving them to friends and keeping a note of who they have given them to. This can help protect the student's number from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

### *5.1.2 Mobile phone - Unacceptable Uses*

- Unless express permission is granted (as outlined above for exceptions), mobile phones should not be with students or in their bags, used to make calls, send SMS messages, surf the internet, take photos or use any other application during School hours or during extra-curricular activities.
- Using mobile phones to bully and threaten other students is unacceptable and will not be tolerated. In some cases it can constitute criminal behaviour.
- Students will not 'gang up' on another student and use their mobile phones to take videos and pictures of acts to denigrate and humiliate that student and then send the pictures to other students or via social media or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student without their consent.
- It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.
- Mobile phones are not to be with students or in their bags, used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the School.

### *5.1.3 Inappropriate Conduct*

- Any student/s caught using a mobile phone to cheat in exams or assessments will face disciplinary action as sanctioned by the Principal.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone in conjunction with the School community will face disciplinary action as sanctioned by the Principal.
- Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using SMS messages, taking/sending photos or objectionable images, and phone calls.
- Students using mobile phones to bully other students will face disciplinary action as sanctioned by the Principal.

## 5.2 Student Laptops/ computers/ iPads

All student laptops are to be used for educational purposes only. Primary school and middle school students are not to bring laptops to school. Middle years students may access school laptops in class under the supervision and direction of their teacher

**Year 10 students**

Year 10 students may bring laptops to school for use in class at the direction of class teachers only. Use of laptops outside the class room is not permitted anywhere on the school grounds

**Use of Laptop Computers by IB senior students**

Year 11 and 12 students are required to bring laptop computers for use in school as bound by the guidelines in this policy.

Students are to use laptops in accordance to their level of study ie: access assigned to them for Managebac.

### *5.2.1 Conditions of Use*

The school must receive a signed permission for student to have an online service account (Appendix A) and a signed acceptable usage agreement for secondary students (Appendix B) before granting students access to online services.

### *5.2.2 Acceptable Usage Agreement*

The school's *Acceptable Usage Agreement* should stipulate that students:

- agree to adhere to the rule's set out in the *Acceptable Usage Agreement* each time they log on to online services;
- ensure that all communication using online services is related to learning or school activities;
- keep passwords confidential, and change them when prompted or when known by another user;
- never knowingly allow others to use their personal online services account unless directed to by a teacher for the purposes of collaborative learning;
- log off at the end of each session to ensure that nobody else can use their online services account;
- not send or publish unacceptable or unlawful material or remarks including offensive, abusive, defamatory or discriminatory comments;
- not access or attempt to access inappropriate material;
- not engage in any bullying, intimidation or other inappropriate behaviour online;
- ask a staff member's advice if another user is seeking excessive personal information, asks to be telephoned, offers gifts by email or wants to meet them;
- immediately tell a nominated staff member if they receive a computer virus or a message that is inappropriate or makes them feel uncomfortable;
- never knowingly initiate or forward emails containing:
    - a message that was sent to them privately;
    - a computer virus or attachments that are capable of damaging recipients' computers;
    - chain letters and hoax emails; and
    - spam like unsolicited advertising material, or mail unrelated to learning;
- be made aware by teachers that emails sent or received via the school's online services may be audited and traced to the online services accounts of specific users;
- not damage or disable computers, computer systems or networks of the school; and
- ensure that online services are not used for unauthorised commercial activities, political lobbying, gambling or any unlawful purpose.

### *5.2.3 Responsible Use of Online Services*

The agreements and forms provided in the appendices are to be used to obtain agreement and sign-off from students and parents. These forms do not constitute or contain legal disclaimers but they do help to meet the requirement to make students and parents aware of their obligations and the risks associated with online services use. Similarly the logon reminder text is to be automatically displayed to all users when logging in to the school network.

The school will periodically repeat requests for sign-off (e.g. at the start of the school year) on the agreements by students and parents as a means of reminding them of their responsibilities when using the school's information and communication technologies.

Monitoring and tracking online activity across the school's network is a complex activity. It is important therefore to realise that it will not always be possible for ICT staff to trace online activity or to provide comprehensive historical details of individual online activity.

## 5.3 Breaches of online communication, mobile phone and digital technology usage

Breach of expectations related to use of online communication and/or services, mobile phones, interactive & digital technologies are managed in a step by step process.

A breach of expectations means there are important issues of trust and responsibility that must be addressed, and students can expect consequences and a follow up process for any such breaches.

Continued breaches will be considered a behavioural matter and the student can expect some or all of the following consequences to apply, depending on the nature and seriousness of the breach:

- Confiscation - removal of device
- Community service
- Suspension

Process for confiscation of devices:

1. First occasion - Device will be sent to the front desk to be collected at the end of the day.
2. Second occasion - Device will be handed to the front desk at the start of each day for 2 days and collected at the end of each day.
3. Third occasion - Device will be handed to the front desk and the student's parent will be required to pick it up.

   This will also result in the student having a conversation and follow up behaviour management plan implemented by the Principal or their delegate as per section 5.4.1

   Repeated infringements may result in the withdrawal of the agreement to allow the student to bring the mobile telephone to School and disciplinary action including suspension may be imposed.

### *5.3.1 Misuse and Breaches of Acceptable Usage*

The Principal and teachers will endeavour, with due regard to practical considerations, to:

- follow procedures for fairness and due process where there is an alleged misuse or breach of this policy including investigating any reported misuse and, where possible, accurately retracing misuse to the offender;
- tailor disciplinary action taken in relation to students to meet specific concerns related to the breach, and assist students in gaining the self-discipline necessary to behave appropriately when using the online services; and
- promptly address the online publication of defamatory material about staff members or students.

## 5.4 Privacy, access and security

The Principal will endeavour, with due regard to practical considerations, to:

- inform parents and teachers of this policy's existence;
- provide students access to online services-enabled computers within the limits of available resources;
- advise parents that while Sophia Mundi Steiner School will make every reasonable effort to provide a safe and secure online learning experience for students when using the school's online services, it is not possible to guarantee that students will not be exposed to inappropriate material;
- advise parents that any internet browsing by their child at home or from other non-school locations, will not be via the school's online services and therefore will not be filtered by the school; and
- approve any material planned for publication on the internet or intranets and verify appropriate copyright and privacy clearance.

Teachers will endeavour, with due regard to practical considerations, to:

- provide appropriate supervision for students using the internet and other online services at school; and
- issue and maintain student passwords in a confidential and secure manner, with additional consideration and provision given to special needs students.

### *5.4.1 Filtering*

The school provides a level of content filtering through its basic list of banned sites service. This lists and bans access to sites that have been identified as unsuitable for the education market. Teachers should notify the Principal of any additional sites which they consider inappropriate and wish to have added to the school's list of banned sites.

### *5.4.2 Intellectual Property and Copyright*

Students need to:

- be aware of the legal requirements regarding copyright when downloading information;
- gain permission before electronically publishing users' works or drawings;
- always acknowledge the creator or author of any material published;
- observe appropriate copyright clearance including acknowledging the author or source of any information used; and
- ensure any material published on the internet or intranet has the approval of the Principal.

### *5.4.3 Student image protection and personal information - Privacy and Confidentiality*

The Principal will endeavour to gain written permission from the student or their parent if the student is under 18 years of age, before publishing video recordings, photographs or comments relating to their students.

Teachers will where possible advise students they should not reveal personal information including names, addresses, financial details (e.g. credit card), telephone numbers or images (video or photographic) of themselves or others.

***Guidelines***

*The school address or email address may be used where it is necessary to receive a reply.*

*Students should also be aware that, since their online services email address contains their personal name, this address should also be protected and should never be used in non-school online communications.*

*Further information on the importance of online anonymity and protective online behaviours is available at: http://www.netalert.gov.au*

## 5.5 Guidelines for Teachers - Use of online communication, mobile phones, and interactive & digital technologies

It is recommended that teachers:

- are aware of their responsibilities for supervising student use of online services as laid out in this policy and the *Duty of Care Policy*;
- maintain an informed view of the relative risks and educational benefits of online activity by their students;

  *Guidelines*

  *A variety of resources are available from NetAlert (www.netalert.gov.au) to assist with this including wall charts, quick reference guides and detailed background information.*
- ensure that students are aware of the possible negative consequences of publishing identifying information online including their own or other students' images;
- refrain from publishing student images or any student-identifying information on the internet (if such publication is necessary, limit the amount of time the information is online as much as possible);
- check that any material planned for publication on the internet or intranets has the approval of the Principal and has appropriate copyright and privacy clearance;
- are aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public, including:
    - collecting as much information as possible about the incident including copies of communications;
    - emphasising to the student that the event is not necessarily their fault;
    - identifying any risky behaviours on the part of the reporting student and counselling them on the need to adopt more protective behaviours; and
    - if the incident warrants further attention, escalate it to the Principal, notifying police only if you suspect the law may have been broken, such as a possible attempt by an adult to groom or encourage the student to meet face-to-face;
- inform parents that student internet access from home or other non-school sites does not occur via the school's online services and therefore internet browsing may not be filtered;
- promote the use of strong passwords for students who can cope with the complexity, these passwords:
    - contain a mixture of alphabetic and non-alphabetic characters;
    - are changed frequently;
    - do not contain dictionary words;
    - do not contain easily identified personal information such as name, date of birth, etc;
    - do not contain any part of the account identifier such as the username; and
    - are not written down.
- adapt the *Acceptable Usage Agreement* to suit the class context and the needs of students (in particular, giving consideration to the value of having students with disabilities signing an agreement).

### *5.5.1 Guidelines for Practical Use of Online Services*

It is recommended that **the** Principal and teachers:

- set realistic expectations with students prior to use of online services, for example when they can expect email replies;
- use mail enabled groups and list services to facilitate communication within the school;
- encourage users to manage their mailbox, deleting unnecessary email and backing up important emails or attachments; and
- encourage users to avoid submitting large attachments to forums and email list services.

## 5.6 Theft or Damage

- Students should mark their mobile phone clearly with their names.
- Students who bring a mobile phone to School should leave it at the mobile drop-in at the office when they arrive.
- Mobile phones that are found in the School and whose owner cannot be located should be handed to the School office.
- The School accepts no responsibility for replacing lost, stolen or damaged mobile phones.
- The School accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from School.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.
- Lost and stolen mobile phones in Australia can be blocked across all networks making them virtually worthless because they cannot be used.

## 5.7 Student Exchange Programme requirements

Sophia Mundi will ensure that exchange students and their host families are informed of the need for to protect their personal privacy, and the privacy of members of their host family. This includes the appropriate use and risks of the internet and social media platforms such as Facebook, Twitter, Instagram, YouTube, Snapchat, TikTok, Weibo, WeChat, or WhatsApp.

# 6 Legal and regulatory basis for compliance

Sophia Mundi employees, students, visitors, volunteers and contractors are required to act in accordance with relevant legislation:

- *Education and Training and Reform Act 2006 (Vic)*
- *Equal Opportunity Act 2010 (Vic)*
- *Education and Training Reform Regulations 2007*
- *Education and Training Regulations 2017*
- *Australian Education Amendment Act 2017*
- *Equal Opportunity Act 1995*

*Child Safe Standards legislation*

a. Child Wellbeing and Safety Act (Vic)
b. Ministerial Order 870 January 2016 (Vic)
c. Crimes Act 1958 (amended) (Vic)
d. Betrayal of Trust Report 2014 (Vic)
e. Working With Children Act 2005 (Vic)
f. Wrongs Amendment (Organisational Child Abuse) Act 2017 (Vic).
g. Disability Discrimination Act 1992
h. Disability Standards for Education 2005

- *Privacy Act 1988 (Cth.)*
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth.)*

# 7 Roles and responsibilities

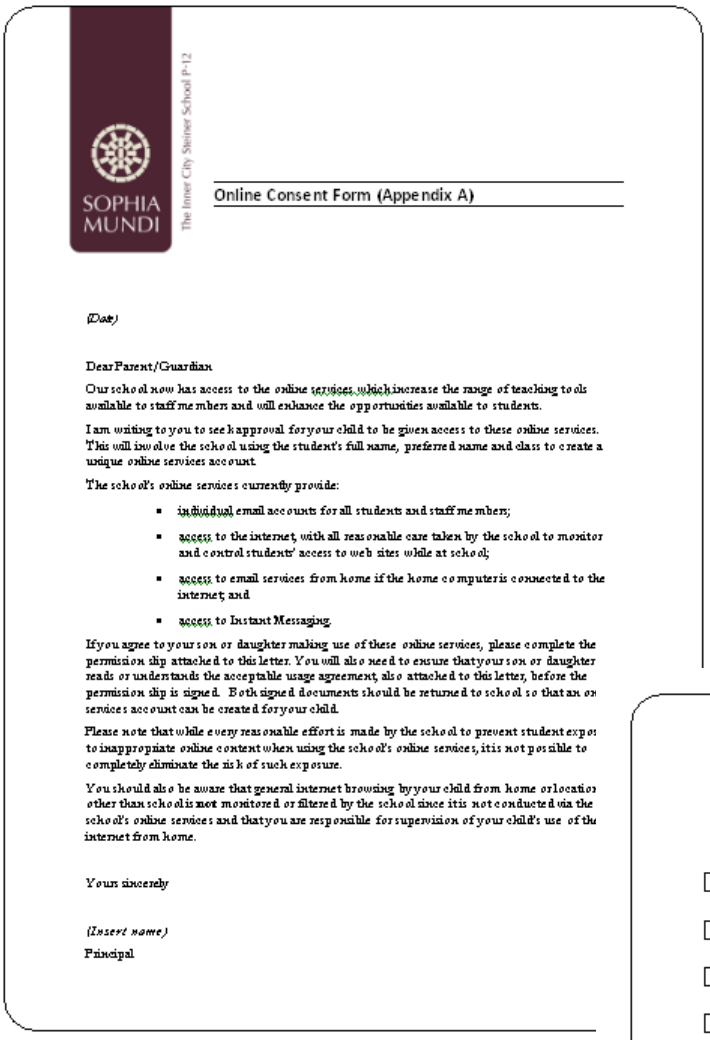
Relevant school policies and procedures:

- Duty of care
- Student engagement and wellbeing
- Positive learning strategy
- Privacy

Students, staff or parents can report any breaches of the enclosed User Agreements or incidents of cyber bullying activity in relation to online communication, mobile phones, interactive & digital technologies to a staff member or Principal at any time.

The Principal and teachers have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen within the online learning environment.

# Appendix A Online Consent Form



SOPHIA MUNDI

The Inner City Steiner School P-12

Online Consent Form (Appendix A)

*(Date)*

Dear Parent/Guardian

Our school now has access to the online services which increase the range of teaching tools available to staff members and will enhance the opportunities available to students.

I am writing to you to seek approval for your child to be given access to these online services. This will involve the school using the student's full name, preferred name and class to create a unique online services account.

The school's online services currently provide:

- individual email accounts for all students and staff members;
- access to the internet, with all reasonable care taken by the school to monitor and control students' access to web sites while at school;
- access to email services from home if the home computer is connected to the internet; and
- access to Instant Messaging.

If you agree to your son or daughter making use of these online services, please complete the permission slip attached to this letter. You will also need to ensure that your son or daughter reads or understands the acceptable usage agreement, also attached to this letter, before the permission slip is signed. Both signed documents should be returned to school so that an online services account can be created for your child.

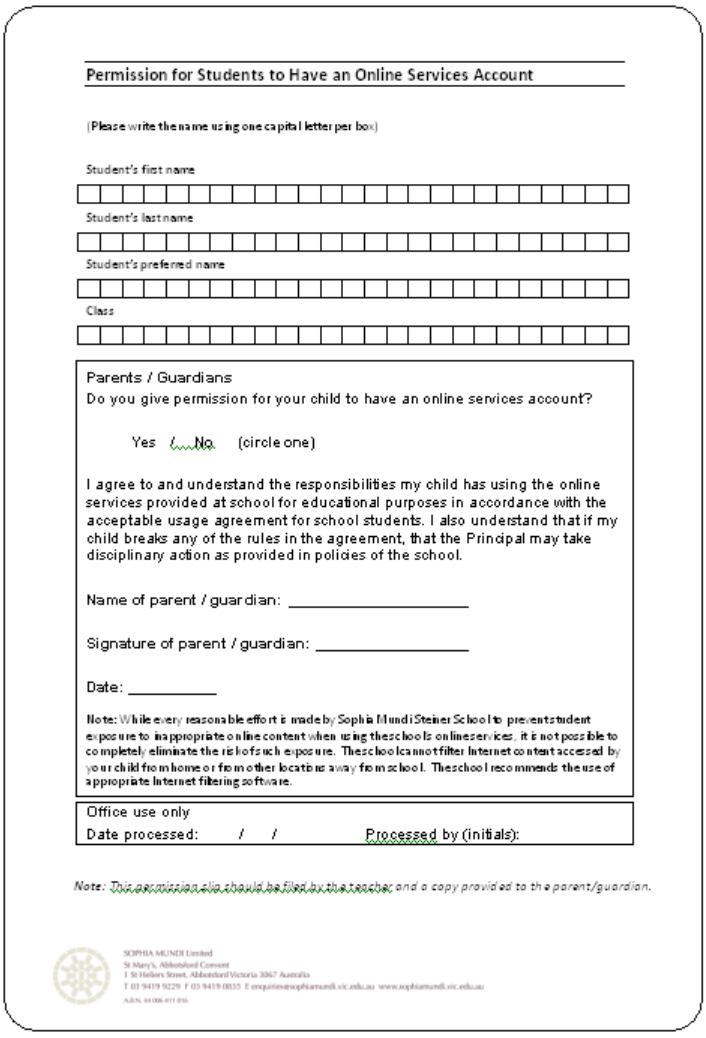
Please note that while every reasonable effort is made by the school to prevent student exposure to inappropriate online content when using the school's online services, it is not possible to completely eliminate the risk of such exposure.

You should also be aware that general internet browsing by your child from home or location other than school is not monitored or filtered by the school since it is not conducted via the school's online services and that you are responsible for supervision of your child's use of the internet from home.

Yours sincerely

*(Insert name)*

Principal



Permission for Students to Have an Online Services Account

(Please write the name using one capital letter per box)

Student's first name

Student's last name

Student's preferred name

Class

Parents / Guardians

Do you give permission for your child to have an online services account?

Yes / No (circle one)

I agree to and understand the responsibilities my child has using the online services provided at school for educational purposes in accordance with the acceptable usage agreement for school students. I also understand that if my child breaks any of the rules in the agreement, that the Principal may take disciplinary action as provided in policies of the school.

Name of parent / guardian: _____

Signature of parent / guardian: _____

Date: _____

Note: While every reasonable effort is made by Sophia Mundi Steiner School to prevent student exposure to inappropriate online content when using the school's online services, it is not possible to completely eliminate the risk of such exposure. The school cannot filter Internet content accessed by your child from home or from other locations away from school. The school recommends the use of appropriate Internet filtering software.

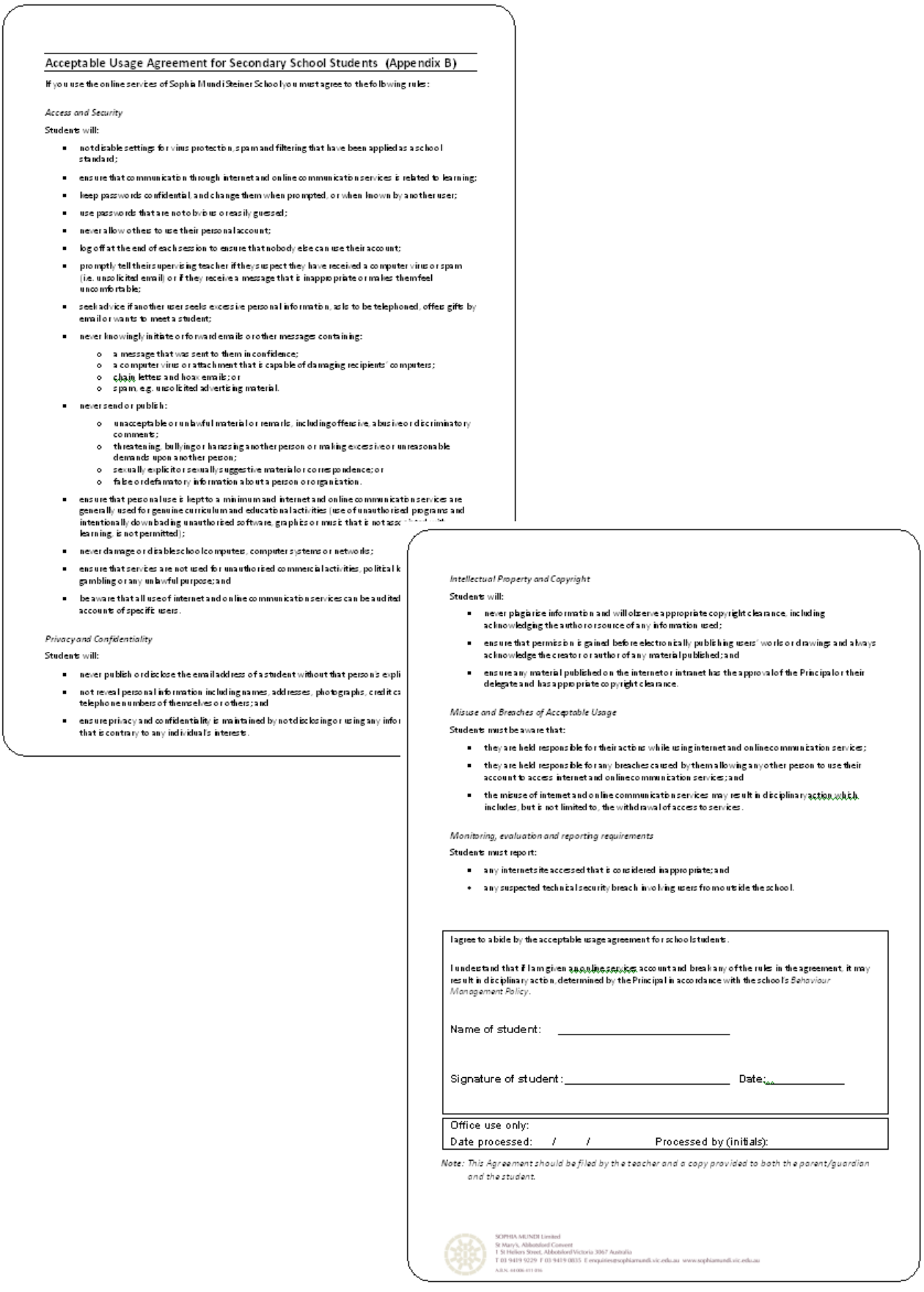
Office use only

Date processed: / / Processed by (initials):

*Note: This permission slip should be filed by the teacher and a copy provided to the parent/guardian.*

SOPHIA MUNDI Limited
St Mary's, Abbotsford Convent
1 St Heliers Street, Abbotsford Victoria 3067 Australia
T 03 9419 9229 F 03 9419 0855 E enquiries@sophiamundi.vic.edu.au www.sophiamundi.vic.edu.au
A.B.N. 64 006 811 856

# Appendix B Acceptable Usage Agreement for Secondary School Students



## Acceptable Usage Agreement for Secondary School Students (Appendix B)

If you use the online services of Sophia Mundi Steiner School you must agree to the following rules:

*Access and Security*

Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a school 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 account;
- log off at the end of each session to ensure that nobody else can use their 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; or
  - 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; or
  - false or defamatory information about a person or organization.
- ensure that personal use is kept to a minimum and internet and online communication services are 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 school computers, computer systems or networks;
- ensure that services are not used for unauthorised commercial activities, political lobbying, gambling or any unlawful purpose; and
- be aware that all use of internet and online communication services can be audited and accounts of specific users.

*Privacy and Confidentiality*

Students will:

- never publish or disclose the email address of a student without that person's expli
- not reveal personal information including names, addresses, photographs, credit ca telephone numbers of themselves or others; and
- ensure privacy and confidentiality is maintained by not disclosing or using any infor 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 and always acknowledge the creator or author of any material published; and
- ensure any material published on the internet or intranet has the approval of the Principal or their delegate and has appropriate copyright clearance.

*Misuse and Breaches of Acceptable Usage*

Students must be aware that:

- they are held responsible for their actions while using internet and online communication services;
- they are held responsible for any breaches caused by them allowing any other person to use their account to access internet and online communication services; and
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

*Monitoring, evaluation and reporting requirements*

Students must report:

- any internet site accessed that is considered inappropriate; and
- any suspected technical security breach involving users from outside the school.

I agree to abide by the acceptable usage agreement for school students.

I understand that if I am given an online service account and break any of the rules in the agreement, it may result in disciplinary action, determined by the Principal in accordance with the school's *Behaviour Management Policy*.

Name of student: _____

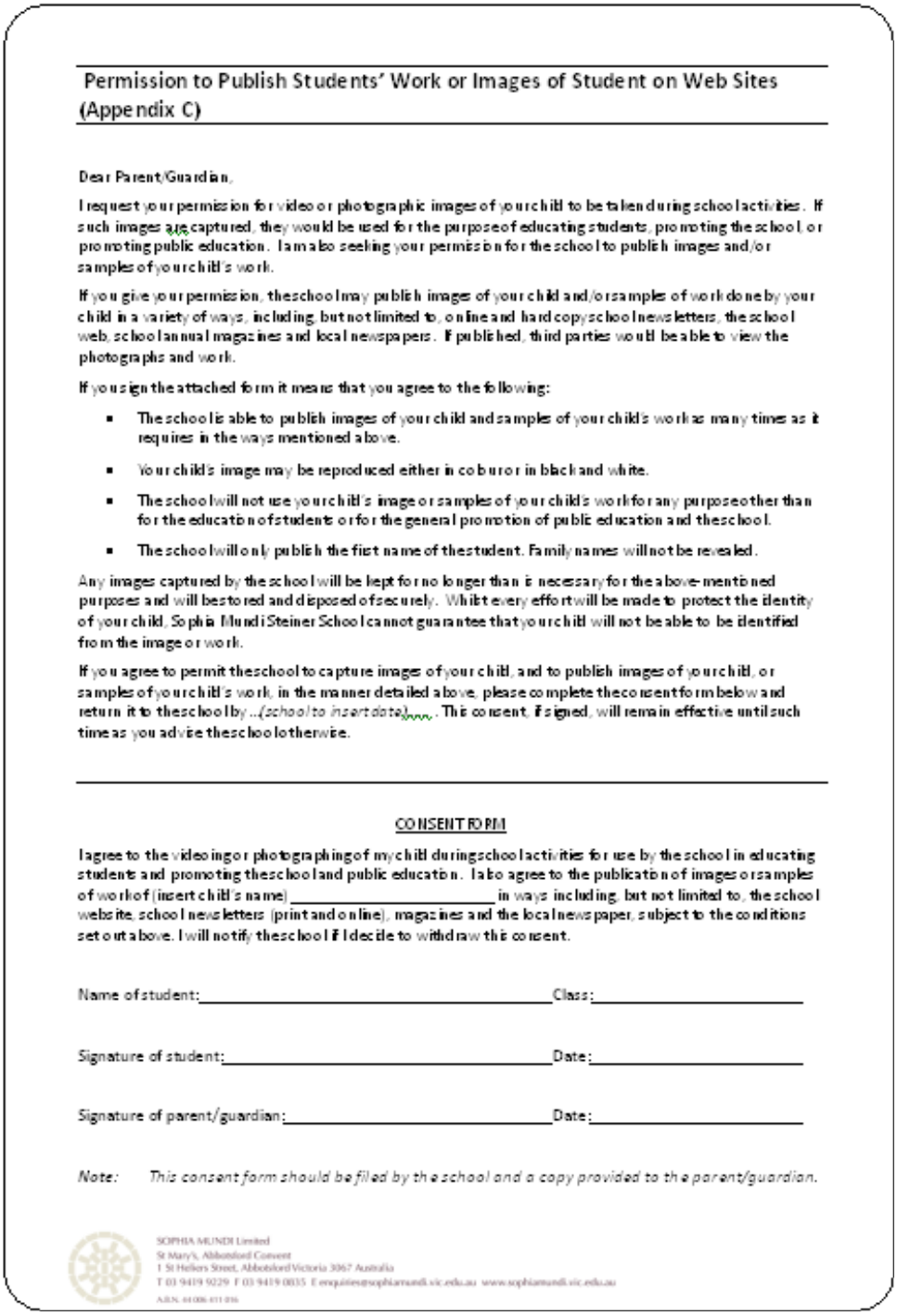
Signature of student: _____ Date: _____

Office use only:
Date processed: / / Processed by (initials):

*Note: This Agreement should be filled by the teacher and a copy provided to both the parent/guardian and the student.*

SOPHIA MUNDI Limited
St Mary's, Abbotsford Convent
1 St Heliers Street, Abbotsford Victoria 3067 Australia
T 03 9419 9229 F 03 9419 0835 E enquiries@sophiamundi.vic.edu.au www.sophiamundi.vic.edu.au
ABN: 44 006 431 036

## Appendix C Permission to Publish Students' Work or Images of Student on Web Sites



Permission to Publish Students' Work or Images of Student on Web Sites (Appendix C)

Dear Parent/Guardian,

I request your permission for video or photographic images of your child to be taken during school activities. If such images are captured, they would be used for the purpose of educating students, promoting the school, or promoting public education. I am also seeking your permission for the school to publish images and/or samples of your child's work.

If you give your permission, the school may publish images of your child and/or samples of work done by your child in a variety of ways, including, but not limited to, online and hard copy school newsletters, the school web, school annual magazines and local newspapers. If published, third parties would be able to view the photographs and work.

If you sign the attached form it means that you agree to the following:

- The school is able to publish images of your child and samples of your child's work as many times as it requires in the ways mentioned above.
- Your child's image may be reproduced either in colour or in black and white.
- The school will not use your child's image or samples of your child's work for any purpose other than for the education of students or for the general promotion of public education and the school.
- The school will only publish the first name of the student. Family names will not be revealed.

Any images captured by the school will be kept for no longer than is necessary for the above-mentioned purposes and will be stored and disposed of securely. Whilst every effort will be made to protect the identity of your child, Sophia Mundi Steiner School cannot guarantee that your child will not be able to be identified from the image or work.

If you agree to permit the school to capture images of your child, and to publish images of your child, or samples of your child's work, in the manner detailed above, please complete the consent form below and return it to the school by *...(school to insert date)*. This consent, if signed, will remain effective until such time as you advise the school otherwise.

CONSENT FORM

I agree to the videoing or photographing of my child during school activities for use by the school in educating students and promoting the school and public education. I also agree to the publication of images or samples of work of (insert child's name) _____ in ways including, but not limited to, the school website, school newsletters (print and online), magazines and the local newspaper, subject to the conditions set out above. I will notify the school if I decide to withdraw this consent.

Name of student: _____ Class: _____

Signature of student: _____ Date: _____

Signature of parent/guardian: _____ Date: _____

*Note: This consent form should be filed by the school and a copy provided to the parent/guardian.*

SOPHIA MUNDI Limited
St Mary's, Abbotsford Convent
1 St Heliers Street, Abbotsford Victoria 3067 Australia
T 03 9419 9229 F 03 9419 0835 E enquiries@sophiamundi.vic.edu.au www.sophiamundi.vic.edu.au
A.B.N. 84 006 411 016

## Appendix D Logon Reminder Notice

The notice shown below, or some variation of this notice, will be displayed to all students when logging into Sophia Mundi Steiner School's online services:

**Appropriate Use of Online Services**

Sophia Mundi Steiner School's online services such as e-mail, internet access, instant messaging and learning services are provided to assist you in your education.

By using these services you agree to obey the rules set out in the Acceptable Usage Agreement and to abide by the school's policies. You also give consent to logging, monitoring, auditing and disclosure of your use of these services.

Inappropriate use of these services can result in disciplinary action that may include suspension of access to services.

Q: How can I help my child get the best out of the net?
Q: What risks should I know about and how do I protect my child on the net?
Q: How do I make a complaint about offensive material?
Q: Where can I find great sites for kids?

www.cybersmart.gov.au

If you would like to talk to us in your own language, please call the Telephone Interpreter Service on 131 450 and they will contact us for you.

ITALIAN
Se desiderate parlare con noi in italiano, siete pregati di chiamare il servizio d'interpretariato telefonico (Telephone Interpreter Service) al numero 131 450 e loro ci contatteranno per voi.

VIETNAMESE
Nếu quý vị muốn nói chuyện với chúng tôi bằng tiếng Việt, xin điện thoại đến Dịch vụ Thông dịch qua Điện thoại (TIS) ở số 131 450 và họ sẽ giúp quý vị liên lạc chúng tôi.

GREEK
Αν θέλετε να μας μιλήσετε στη γλώσσα σας, παρακαλείστε να τηλεφωνήσετε στην Τηλεφωνική Υπηρεσία Διερμηνέων στο 131 450 και να ζητήσετε να επικοινωνήσουν μαζί μας εκ μέρους σας.

ARABIC
إذا كنت تودّ التحدث إلينا بلغتك، فيرجى الاتصال بخدمة الترجمة الشفهية والخطية على الرقم 450 131 حيث يقوم مترجم من الخدمة بالاتصال بنا والتحدث إلينا نيابةً عنك.

CHINESE
如果您希望用您的語言和我們傾談，請致電 131 450 電話傳譯員服務 (Telephone Interpreter Service)，他們會替您和我們聯絡。

Produced by the Australian Communications and Media Authority and endorsed by all Australian law enforcement authorities


For more information contact:
Australian Communications and Media Authority
Cybersafety Contact Centre
Telephone: 1800 880 176
Email: cybersafety@acma.gov.au

June 2009

www.cybersmart.gov.au

acma

cyber(smart:)

# CYBERSMART GUIDE to internet safety

Australian Communications and Media Authority

Children need parents and family members to help them become Cybersmart!

# Cybersmart tips for parents

Help your kids to make smart choices about who and what they find online. To do so:

### Spend time online

The internet can be a fun family activity—check out good sites with your kids! Compile a favourites list, which you can visit again and again.

### Help your children use the internet as an effective research tool

Learn about handy homework tips for kids and also good searching ideas.

### Teach children that information on the internet is not always reliable

If it sounds too good to be true, it probably is!

### Teach your children 'netiquette'

Encourage them to treat others online in the same way they should in real life.

### Set rules

Make sure your children know what information they can give out and where they can go on the net. Limit time in chat rooms, particularly for younger children. Encourage the use of chat rooms that are moderated (that is, where messages are screened by an adult before they are made public).

### Chat safely—be aware of strangers online

Chatting on the net is very popular among young people, particularly young teenagers. It can be a great way to meet and talk with people across borders, time zones and backgrounds.

However, a lot of real world risks also exist online, especially in chat rooms. Most people online are friendly and polite but some can be unfriendly and rude. A small number are exploitative and predatory. Be aware of this and encourage your children not to respond to any communication that makes them uncomfortable.

### Be involved

Put the internet computer in a public area of the home. Areas like the living room are ideal, rather than a child's bedroom.

Talk to your children about their experiences online—the good and the bad. Get to know which chat rooms they are visiting and who they are chatting with.

### Talk to your children

Let them know it's okay to tell you if they come across something that worries them. It doesn't mean that they're going to get into trouble.

If your child wants to meet someone they have met online, you should find out about the person to see that they are who they say they are. Talk to them and their parents by phone first and accompany your child to the meeting.

### Teach your kids ways of dealing with disturbing material

Explain that they should not respond if someone says something inappropriate and they should immediately leave any site if they feel uncomfortable.

Encourage them to tell you if anyone says something that makes them feel uncomfortable or scared.

**Remember!**
**The best protection is parental supervision and guidance.**

# Chatsmart

## KIDS: These tips are for you!

### Be careful

Meeting people online might be fun, but remember that the people you meet online may not be who they say they are. Someone claiming to be a 12-year-old girl could really be a 40-year-old man.

### Check with your parents/carer first

Ask your mum, dad or carer before you give out your name, phone number or address or any other personal details. This includes the name of your school, your photo and any personal information about your friends and family. Never post such information in a chat room or somewhere lots of other people might see it.

Always keep your password a secret.

### Take someone with you

If you want to meet someone you have so far only met in a chat room, ask one of your parents or another trusted adult to go with you. Always meet in a popular public place, preferably during the day.

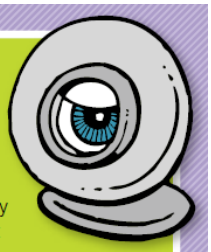
### Don't stay. Don't respond

If someone in a chat room posts offensive pictures or says something rude or scary, or if you are sent these in an email, don't respond, save it and leave the chat room straightaway.

### Tell

If you see upsetting language, nasty pictures or something scary tell your parent or another adult you trust.

# Webcam



### Keep it quiet!

Only tell real-life friends or family that you have a webcam. Don't show it in your online ID.

### Say NO!

If someone asks you to do or watch something that you find upsetting or wrong say NO! Close the conversation straight away and tell your parent or another adult that you trust.

## Be IM smart too!


### Be careful!

ONLY add friends you really know to your contact list!

### Remember!

You can block strangers from seeing when you are online!

# Spam

Spam is electronic 'junk mail'—unwanted messages sent to your email account or mobile phone. Spam may contain offensive material, malicious code, try to persuade you to buy a product or service or attempt to trick you in to divulging your banking details. The best response is to delete and never respond to spam messages.

To reduce spam, protect your email address and mobile phone number online, use filtering software and boost your internet security. Also check your internet service provider's website for information about managing spam. Complaints about spam should be made online at **www.acma.gov.au/spam**.

# Filters

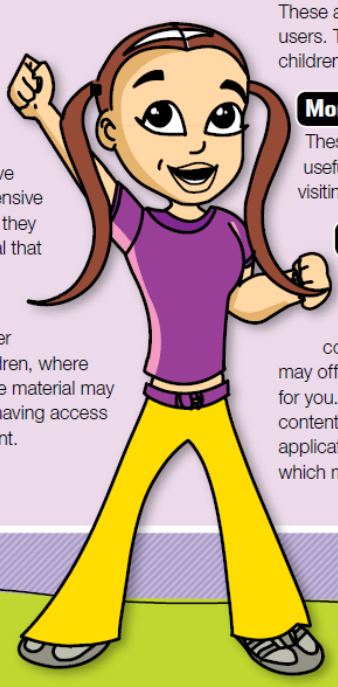
Filter software is a useful tool for managing children's access to the net, along with active supervision by parents and setting household internet-use rules.

Different filters work in different ways. Some are better than others at blocking particular types of content.

### Whitelist filters

These allow the user to access only a selected number of pre-determined sites while blocking all others. They are the most effective in blocking access to offensive and harmful material, but they also block a lot of material that may be innocuous.

These filters are likely to be appropriate for younger (primary school age) children, where protection from unsuitable material may be more important than having access to a wider range of content.



### Blacklist filters

These prevent the user from accessing certain listed sites. They provide access to a wider range of content, but may still allow access to unsuitable material and block legitimate material. Such filters are likely to suit families with older children, where access to a wide range of content is an important consideration.

### Multiple user filters

These allow different levels of filtering for different users. They may be useful where there are children of different ages in the family.

### Monitoring filters

These keep a record of visited sites and can be useful for checking the sites your children are visiting on the net.

### Points to remember

To help ensure your filter is as effective as possible, consider installing a product that is updated automatically when you connect to the net. Alternatively, your ISP may offer a filter that they administer and update for you. Some filters work only with WWW content, others can be used with a wider range of applications such as email or chat. Look for one which meets your particular needs.

### More information

The ACMA has a code of practice for internet service providers (ISPs). This requires them to offer each subscriber one of the filters listed in the code. Some ISPs offer this service free of charge, while others charge a fee. See your ISP's home page for details of the product they offer. The Internet Industry Association provides a list of family-friendly internet content filters on its site at **www.iia.net.au**.

### HOTLINE

If you see content on the net that you believe may be prohibited, you can make a complaint to the ACMA about it. Complaints should be made online at **www.acma.gov.au/hotline**.

**REMEMBER**
**A filter cannot be a substitute for parental supervision.**

**www.cybersmart.gov.au**

# ISV - Cyber safety Information Sheet

## Cyber safety

Cyber safety is the responsible and safe use of communications and information technology. It involves keeping personal information secure and safe, being responsible with that information, being respectful of other internet users, and using good internet etiquette (netiquette).

## Cyber bullying

Cyber bullying is the use of technology to harass, threaten, embarrass or target another person.

### Risks

Risks can include:

- peer pressure to be engaged with friends through social media
- accessing and/or sharing inappropriate, disturbing, explicit or illegal content
- contact with strangers: the potential for online grooming and radicalisation
- posting private information that, by posting, becomes public
- 'using (or stealing) content owned by others, e.g. images, music or videos
- Plagiarising: taking ideas or information created/owned by others without referencing their origin
- not using critical thinking skills when using the internet'[1]
- not seeking or not knowing how to seek support from someone in real life when there is an issue
- potential increase in mental health issues or social isolation
- lack of ethical decision making (difference between what is right and wrong) and appropriate standards of behaviour
- creating a digital footprint that may be permanent
- covert bullying: the potential for anonymity may result in an increase in online bullying as those who bully and those who are bullied may choose to retaliate online rather than face-to-face
- sexting: sending sexually explicit messages or photographs via the internet, mobile phones and other forms of social media.

### Cyberbullying versus Traditional Bullying

Cyber bullying differs from traditional bullying in several ways:

- **Availability:** cyber bullying can occur anywhere and at any time. There is a misperception that there are no real-world consequences for online actions.
- **Anonymity:** the impression of anonymity in the 'online world' leads young people to feel less accountable for their actions and provides a false bravado to would-be bullies.
- **Geography:** rather than being limited to the schoolyard, cyber bullying can operate wherever a young person uses the internet or a mobile phone, including when they are on their own in their bedroom and at night.
- **Impact:** the internet provides the means for 'bullying' to be available to a wide audience and instantaneously. Through social media sites, comments and photos can be viewed by potentially an unlimited number of people.
- **Intent:** a private message or joke that is forwarded on may become offensive or harassing, even though that may not have been the intention of the original sender.
- **Permanence:** verbal comments are fleeting. Online content is tracked and stored and can potentially resurface at any time.
- **Democracy:** anyone can be a victim – students, staff, and parents.


## Extra tips for PARENTS

**Do you know who your kids are talking to?**

**Stay involved** with your child's use of new technologies. Ask your child to show you how his or her phone works, or borrow it and become familiar with it.

**Find out** how access to 'adult' content and other services offered by your child's mobile phone carrier can be managed. Such information is usually available on the carrier's website.

**Talk** to your children about their experiences the good and the bad. Let them know it's OK to tell you if they come across something that worries them. (It doesn't mean they're going to get into trouble.)

**Teach** your children that there are ways they can deal with disturbing material—they should not respond if they are sent something inappropriate, and they should immediately leave or hang up if they feel uncomfortable or worried by it.

www.cybersmart.gov.au

If you would like to talk to us in your own language, please call the Telephone Interpreter Service on 131 450 and they will contact us for you.

**ITALIAN**
Se desiderate parlare con noi in italiano, siete pregati di chiamare il servizio d'interpretariato telefonico (Telephone Interpreter Service) al numero 131 450 e loro ci contatteranno per voi.

**VIETNAMESE**
Nếu quý vị muốn nói chuyện với chúng tôi bằng tiếng Việt, xin điện thoại đến Dịch vụ Thông dịch qua Điện thoại (TIS) ở số 131 450 và họ sẽ giúp quý vị liên lạc chúng tôi.

**GREEK**
Αν θέλετε να μας μιλήσετε στη γλώσσα σας, παρακαλείστε να τηλεφωνήσετε στην Τηλεφωνική Υπηρεσία Διερμηνέων στο 131 450 και να ζητήσετε να επικοινωνήσουν μαζί μας εκ μέρους σας.

**ARABIC**
إذا كنت تودّ التحدث إلينا بلغتك، فيرجى الاتصال بخدمة الترجمة الشفهية والخطية على الرقم 131 450 حيث يقوم مترجم من الخدمة بالاتصال بنا والتحدث إلينا نيابةً عنك.

**CHINESE**
如果您希望用您的語言和我們傾談，請致電 131 450 電話傳譯員服務 (Telephone Interpreter Service)，他們會替您和我們聯絡。

For more information contact:
Australian Communications and Media Authority
Cybersafety Contact Centre
Telephone: 1800 880 176
Email: cybersafety@acma.gov.au

June 2009

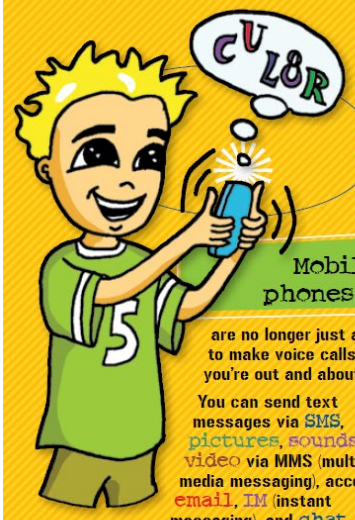
www.cybersmart.gov.au

acma

cyber(smart:)

## How to be PHONE SMART (and stay safe)

# Cybersmart tips for kids and young people




**Mobile phones** are no longer just a way to make voice calls when you're out and about.

You can send text messages via SMS, pictures, sounds, video via MMS (multi-media messaging), access email, IM (instant messaging), and chat, as well as surf the net.

Many mobiles include cameras, sound recording capability, and can also track where you are! While most content and services will be suitable for everyone, some may be unsuitable and risky for kids.

The 'always on' nature of mobile services means that risks, such as cyberbullying, people making inappropriate contact and the chance that kids will access unsuitable content, are always present.

They can happen at any time, anywhere. And because parents can't always be there to supervise, it is more important than ever to teach kids how to protect themselves.

**Do you REALLY know who you're talking to?**

Keep **secrets**—don't tell anyone your personal details. This includes your name, address, your current location, credit card details and school. Be very careful about giving out your phone number too.

**Check** with your Mum, Dad or carer before you give anyone this information, particularly to people who you may have only just met online.

**Remember**—the person you meet in a chat room may not be who they say they are. And if you give out personal information or send pictures, the person you send them to may not be the only person to see them!

Take **someone** with you. If you want to meet someone you haven't met so far in person, ask a parent or another adult to go with you and always meet in a popular public place, preferably during the day.

Say **NO**! Don't accept any offers that seem too good to be true—they probably are. Never accept the offer of a free mobile phone from someone without asking your Mum or Dad first!

**Watch out!** Stay aware of what's going on around you and guard your privacy. Remember, if you can take pictures of everything and everyone with your phone, so can other people ... and you may not want to be the subject of their photos!

Be **considerate**—only send the kinds of messages and pictures you would be happy to receive.

**Tell**—if someone sends you nasty or bullying messages, or asks you to do something that makes you feel uncomfortable, don't respond. Make a note of the number it came from, and the date and time of the call, save the message and tell your parent or another adult you trust.

Remember always to be Phone Smart and stay safe.

**Protect your privacy.**