



SOPHIA
MUNDI

The Inner City Steiner School P-12

Online Communication Policy

Table of Contents

| | | |
|-------------------|---|-----------|
| 1. | Policy..... | 3 |
| 1.1 | Background..... | 3 |
| 1.2 | Scope | 3 |
| 1.3 | Definitions | 3 |
| 1.3.1 | <i>Inappropriate Content</i> | 3 |
| 1.3.2 | <i>Online Services</i> | 3 |
| 1.3.3 | <i>Parent</i> | 3 |
| 1.3.4 | <i>Spam</i> | 3 |
| 1.4 | Relevant Legislation | 3 |
| 2. | Procedures | 4 |
| 2.1 | Access and Security..... | 4 |
| 2.2 | Conditions of Use | 4 |
| 2.3 | Personal Information, Privacy and Confidentiality | 4 |
| 2.4 | Intellectual Property and Copyright | 4 |
| 2.5 | Misuse and Breaches of Acceptable Usage | 5 |
| 3. | Guidelines | 5 |
| 3.1 | Responsible Use of Online Services | 5 |
| 3.1.1 | <i>Acceptable Usage Agreement</i> | 5 |
| 3.2 | Guidelines for Teachers | 6 |
| 3.3 | Guidelines for Practical Use of Online Services | 7 |
| Appendix A | Online Consent Form | 8 |
| Appendix B | Acceptable Usage Agreement for Secondary School Students..... | 9 |
| Appendix C | Permission to Publish Students' Work or Images of Student on Web Sites | 10 |
| Appendix D | Logon Reminder Notice | 11 |
| Appendix E | Cybersmart Guide to Internet Safety | 12 |

1. Policy

Online services provided to students at Sophia Mundi Steiner School will only be used for learning related activities and require informed parental consent and appropriate management.

1.1 Background

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 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 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.

Guidelines

NetAlert is a government-supported internet safety advisory body set up to provide practical information and advice on managing children's access to online content. More information is available from the NetAlert website (www.netalert.gov.au) or by phoning their helpline on 1800 880 176.

1.2 Scope

This policy applies to the Principal, teachers and supervisors of students accessing online services from any of the school's locations including, but not limited to, the school.

1.3 Definitions

1.3.1 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.

1.3.2 Online Services

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

1.3.3 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.

1.3.4 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.

1.4 Relevant Legislation

- *Copyright Act, 1968*
- *Copyright Amendment (Digital Agenda) Act 2000*

- *Copyright Amendment (Moral Rights) Act 2000*
- *Education and Training Reform Act 2006*
- *Education and Training Reform Regulations 2007*

2. Procedures

2.1 Access and Security

The Principal must:

- 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 must:

- 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.

2.2 Conditions of Use

Teachers 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.

2.3 Personal Information, Privacy and Confidentiality

The Principal must 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 must 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 made 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>

2.4 Intellectual Property and Copyright

Teachers must advise students of the 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.

2.5 Misuse and Breaches of Acceptable Usage

The Principal and teachers must:

- 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.

Teachers must inform students:

- of the consequences of breaches caused by them allowing any other person to use their online services account;
- that the consequences of misusing online services will be withdrawal of access to online services and other consequences outlined in the *Behaviour Management Policy*; and
- of their possible legal liability for offences committed using online services.

Guidelines

Appropriate action by the Principal should be taken in accordance with the Behaviour Management Policy.

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.

3. Guidelines

3.1 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.

3.1.1 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.

3.2 Guidelines for Teachers

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).

3.3 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.

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 Reiner 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 email 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 organisation.
- 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 appropriate for 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 purposes; and
- be aware that all use of internet and online communication services can be audited accounts of specific users.

Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a student without that person's explicit permission;
- not reveal personal information including names, addresses, photographs, credit card or telephone numbers of themselves or others; and
- ensure privacy and confidentiality is maintained by not disclosing or using any information 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' words 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 filed by the teacher and a copy provided to both the parent/guardian and the student.



SOPHIA MUNDI Reiner School
 St Mary's, Altonhills Campus
 1 St Hubert Street, Altonhills Victoria 3087 Australia
 T 03 9419 9229 F 03 9419 0835 E enquiries@sophiamundi.vic.edu.au www.sophiamundi.vic.edu.au
 A.B.N. 61 006 011 916

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.

Appendix E Cybersmart Guide to Internet Safety

- 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, παρακαλούμε να τηλεφωνήσετε στην Τηλεφωνική Υπηρεσία Διεργμένων στο 131 450 και να ζητήσετε να επικοινωνήσουμε μαζί μας εκ μέρους σας.

ARABIC

إذا كنت تودَ 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。

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

Jun e 2009

www.cybersmart.gov.au



cyber(smart:)

CYBERSMART GUIDE to internet safety



Australian Communications and Media Authority

Cybersmart tips for parents



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

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.

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.



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!

+ Add a friend

- ★ gargyle (available)
- ★ misty (available)
- ★ ohsoprettyemma (available)
- ☾ noddy (offline)
- ☾ for-a-good-time-call-jimmeh! (offline)
- ★ napolean37 (away)
- ☾ teh_minx (offline)
- ☾ roisin (offline)
- 🚫 shazza (blocked)
- 🚫 gazza (blocked)
- 🚫 mick99 (blocked)
- ★ sam_the_man (away)

Filters

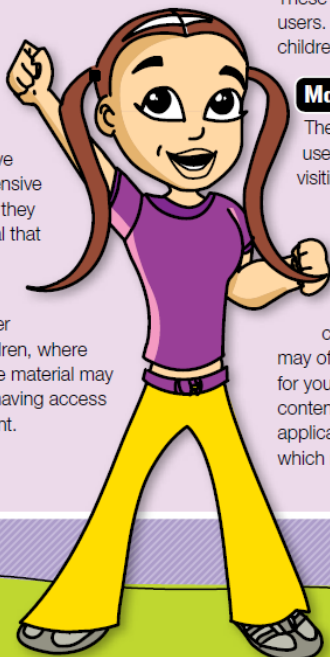
Filter software is a useful tool for managing children's access to the net, along with active supervision by parents and setting household internet-use rules.

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.iaa.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.