



WILD
CHERRY
SCHOOL

For Waldorf/Steiner Education

INTERNET USE 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

1. Policy

Online services provided to students at Wild Cherry School in their final two years of primary 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. Wild Cherry 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 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

eSafety 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 eSafety website (www.esafety.gov.au) or by phoning their helpline on 1800 880 176.

1.2 Scope

This policy applies to the Administration Leader, teachers and supervisors of students accessing online services at 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 Wild Cherry 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 Education and Administration Leaders 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 Wild Cherry 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.

2.2 Conditions of Use

Teachers must receive a signed permission form for students to have an online account if using email and a signed Acceptable Usage Agreement before granting students access to online services.

2.3 Personal Information, Privacy and Confidentiality

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.

Further information on the importance of online anonymity and protective online behaviours is available at:

<http://www.eSafety.gov.au>

2.4 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.

2.5 Misuse and Breaches of Acceptable Usage

The Administration Leader, Education Leader 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.

Teachers will endeavour, with due regard to practical considerations, to 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 Administration Leader or Education Leader 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 Education Leader or Administration Leader 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

Students will be asked to sign an Acceptable Usage Agreement.

3.1.1 Acceptable Usage Agreement

Acceptable usage means that students:

- 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 any personal online services account unless directed to by a teacher for the purposes of collaborative learning;
- 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;
- 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;
- 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 eSAfety (www.eSafety.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 Education Leader and Administration Leader 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 Education Leader and Administration Leader, 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 teachers:

- set realistic expectations with students prior to use of online services, for example when they can expect email replies if email is used;
- 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.