St Albans Secondary College

ICT ACCEPTABLE USAGE POLICY

Guidelines and Conditions for Appropriate Use of Network, Computer and ICT Facilities

EDUCATIONAL RATIONALE:

As we educate our students for a rapidly changing world, we believe it is important for them to learn how to use technology constructively and responsibly.

The St Albans Secondary College network is provided for staff and students to promote educational excellence by facilitating resource sharing, innovation and communication. All students are given full access to the network with an individual account. Students will also have college-administered individual electronic mail and full Internet access. Any such facilities must be regarded as privileges, which may be withdrawn in the case of misuse of the resources.

GENERAL GUIDELINES:

SASC will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning while minimising and managing any risks.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.

The SASC Acceptable Use agreement will cover all College employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment.

The internet, computing facilities and ICT devices / equipment are provided for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

- Access is a privilege, not a right.
- Use of computer/internet resources for educational purposes has priority over other (recreational) uses.
- Appropriate language must be used in all communications including email messages and on web pages.
- The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
- The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.

1. GUIDELINES AND CONDITIONS FOR APPROPRIATE USE OF HARDWARE, SOFTWARE AND INTERNET FACILITIES:

‘Cybersafety’ refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones

‘School ICT’ refers to the school’s computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in below

The term ‘ICT equipment/devices’ used in this document, includes but is not limited to, computers (such as desktops, laptops), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of, video and audio players/receivers (such as portable CD and DVD players) or any other, similar, technologies as they come into use.

A. Computer Hardware/ICT Equipment

Computer / ICT facilities are expensive, sensitive and must be treated carefully.

Students must not:

- Do anything to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment
Students must not, without permission:
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment.

Students are NOT authorised to attempt the repair or adjustment of any college hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to an authorised person.

B. Software and Operating Systems

Students will not:
- Attempt to change any computer settings.
- Bring, download or install unauthorised programs, including games and run them on college computers. Online internet games and the downloading of video material are banned.
- Deliberately introduce any virus or program that reduces system security or effectiveness.

C. Network

Network accounts are to be used only by the authorised owner of the account. It is the responsibility of students to make backup copies of their work. The college will not be held responsible for lost data.

Students must not:
- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Intentionally modify files, other data or passwords belonging to other users.
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Students are responsible for everything done using their accounts, and everything in their home folder.
- Attempt to enter any other person's home directory (W: drive) or do anything whatsoever to any other person's files.
- Store the following types of files in their home directory:
  - Program files (EXE, COM)
  - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)
  - Picture, video or sound files, unless they are required by a subject
  - Obscene material – pictures or text
  - Obscene filenames
  - Insulting material
  - Password-protected files
  - Copyrighted material
  - Games

These files will be removed immediately by the Network Administrator or Computer Technician.

D. Printing

Students must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing. Click here to see Student Printing Limits

E. College Internet Usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. It is not intended for entertainment.

The school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. Filtering software has been placed on Internet links however, it is the responsibility of individual students to ensure their behaviour does not contravene college rules. Click here to see Student Internet Download Limits

F. Email

Throughout the Internet there are accepted practices known as Netiquette, which should be followed. The following points should be noted:
Use appropriate language. Do not be insulting, abusive, swear or use vulgarities.
No messages should contain obscene comments, threats, sexually explicit material or expressions of
bigotry or hate.
Do not reveal your personal address or the phone numbers of students or colleagues.

Note that email is not guaranteed to be private. System administrators do have access to all files including mail.

Students will not:

- send offensive mail
- send unsolicited mail to multiple recipients ("spam")
- send very large attachments - students should check the file size of any attachment as any larger than
  8 mb cannot be sent
- leave mail on the server after it has been read
- use email for any illegal, immoral or unethical purpose
- attempt to disguise their identity or the true origin of their mail
- forge header messages or attempt to use any mail server for deceptive purposes
- use any mail program designed to send anonymous mail
- use Chat lines (IRC, MIRC, ICQ etc) or Real-time chat programs (MIRC, ICQ).

G. World Wide Web

The college will exercise all care in protecting students from offensive material, but the final responsibility must lie
with students in not actively seeking out such material.

Students will not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Violence
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods
- Any other material that the student's parents or guardians have forbidden them to see

If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and
notify a teacher. They must not show their friends the site first.

- The Internet must not be used for commercial purposes or for profit.
- The Internet must not be used for illegal purposes such as spreading computer viruses or
distributing/receiving software that is not in the public domain.
- Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or
programs, which are harmful to another user's data or equipment.
- It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to
transmit another user's document without their prior knowledge and permission. This includes the use of
images and text.

2. Possible Consequences:

The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The
response to individual incidents will follow the procedures developed as part of the school's cybersafety practices.
More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Ban on lunchtime computer use
- Temporary ban on using computers
- Removal of email privileges
- Removal of internet access privileges
- Removal of home directory and network access (with consequent inability to satisfactorily complete unit
requirements of the subject)
- Detention
- Paying to replace damaged equipment
- Removal from classes where computer use is involved
- Suspension from College

Guidelines for the Publishing of Digital Photographs and Student Work on the College Web
and Intranet sites

Written material placed onto the school web site and Intranet must:
be checked for appropriateness and (as far as possible) accuracy
not violate copyright
have the written permission of a parent/guardian if the parent or guardian has requested such a veto
not contain the home address or home phone number of an individual
not contain the e-mail or web address of a student unless specifically required and requested

Publishing of photographs is an important part of recognising the achievements of our students. We are very proud of the work our students do and want to share this work with a wider audience when appropriate, through our Internet (open access) and Intranet (password protected) sites.

To ensure the safety of students it is most important that:

- photographs used are usually group photos
- full names are never published.
- recognisable photos of any student are not published on the Internet site
- only a christian name is included with any work published.

If a student is not happy with a photo that appears on the College intranet (Public drive) or Internet website they can contact the Network Manager and the photo will be removed as soon as possible.

The following section needs to be filled in by the student and his/her parents or legal guardian and returned to the school before internet access is allowed.

ICT ACCEPTABLE USAGE POLICY

AGREEMENT TO ABIDE BY St Albans Secondary College ICT ACCEPTABLE USAGE POLICY
FOR THE USE OF COMPUTER HARDWARE / ICT EQUIPMENT AND SOFTWARE,
INCLUDING THE INTERNET

I agree to follow the College rules for the use of computer hardware, ICT equipment, software and the Internet. I understand that failure to follow the policy above will result in my access being limited. Serious breaches of rules will result in further sanctions. Students banned from the network will be required to make alternative arrangements for completion of set tasks.

STUDENT SIGNATURE ___________________________ DATE ____________

I, the parent or guardian of __________________________ have read and understand the Guidelines and Conditions for Appropriate Use of hardware, Software and Internet Facilities document. I agree that my child shall observe these guidelines and conditions.

PARENT SIGNATURE ___________________________ DATE ____________

DIGITAL PHOTOGRAPHS: INTERNET/INTRANET PUBLISHING PERMISSION FORM

The safety of our students is most important so we do not publish recognisable photos of any student on the Internet site and only include a christian name with any work published.

I give permission for my child’s photograph (generally in a group) and / or examples of high quality student work to be published on the:

<table>
<thead>
<tr>
<th></th>
<th>College Internet Web Site (Visible to the World)</th>
<th>College Intranet Site (Visible only to college members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photograph</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Work</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please consult with your child, then write “Yes” or “No” in the boxes above.

STUDENT SIGNATURE ___________________________ DATE ____________

PARENT SIGNATURE ___________________________ DATE ____________

Evaluation:
This policy will be reviewed as part of the school's three-year review cycle.

This policy was last ratified by School Council in...