Introduction

Information and Communication Technology [ICT] has revolutionised the educational landscape and produced powerful tools for both teaching and learning. The advent of cyberspace in 1991 has produced a digital age of extraordinary power and connective capacity that presents new frontiers not only 'of' education but 'for' education.

While the educational efficiency of ICT enhances cognition and presents considerable gains for student learning, it has the capacity to expose young people to risk associated with cyber-bullying, infringements of copyright, and also the predatory behaviours of those who intentionally misuse the technology for pecuniary or personal gain.

The following Code of Practice aims to address key issues and principles that relate to ICT use in schools and provide teachers and parents with the framework for educating young people for an ethical and productive use of the technology.

The College acknowledges AHISA's Code of Practice – Information and Communications Technology, Cyber Safety and Protection material that provides the basis for much of this policy.

Principles underlining the Information and Communications Technology use at Investigator College

1. That ICT is integral to learning communities in the 21st Century.
2. That all students have proportionate access to the College's ICT provision including hardware and software.
3. That ICT security and safety will be observed by all staff and students.
4. That ICT will be used exclusively for educational and pro-social purposes that are allied to research course of study or positive social interactions.
5. That copyright laws as they apply throughout the Commonwealth will be adhered to at all times.
6. That existing security and safety measures designed to facilitate effective use of ICT in the College be acknowledged and utilised in the College.
7. That issues of privacy as they relate to the Privacy Act 1998 (Privacy Act) and the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 will be respected at all times.
8. That an education program in the school community will support cyber-safety in policy and practice.
9. That authentic sourcing of information to prevent plagiarised information will occur in the production and authentication of student work.
10. That cyber-bullying via errant use of ICT technology will be subject to policy provision and procedure.
11. That violations and/or infringements of ICT use be reported to the appropriate authority or person.

Set out below is the following information:

- ICT Facilities at Investigator College

- ICT Ethics Statement for all users
- Policy on Student use of the Internet [all devices]
- ICT Network Users Contract
- Mobile Phone/Devices

ICT Facilities at Investigator College

The computing facilities at Investigator College are continually expanding and being updated in a uniform fashion across both campuses.

The College has invested in a private wireless backbone network spanning Goolwa, Victor Harbor and Currency Creek. This backbone link carries data, voice and video communications between campuses and enables 'one network'.

All computing equipment is connected to the network with fibre optic between classrooms. Our wireless network is deployed across three campuses to enable devices to automatically connect when within range.

IT equipment deployed across both campuses conform to a 'Standard Operating Environment' with all files saved to servers and tape backup.

The internet connection is filtered using current technology and 'best practice' techniques.

This standardization allows the College to offer identical delivery of curriculum and learning opportunities regardless of location.

ICT Ethics Statement for all users

Ethical behaviour in the use of the computer facilities is required from all who use the network.

Behaviour which is considered inappropriate in terms of the guidelines below may result in the withdrawal of the user's access to the ICT network and any student-owned devices are subject to inspection.

1. Each user may only use the network that has been authorised for their use. If there is password access, the user has a responsibility to maintain secure passwords and take precautions against unauthorised access.
2. Users may only use authorised facilities for authorised purposes.
3. Any attempt to copy software made available for the user's use is prohibited. The College holds a copyright licence to use the software and copying of such material is liable to prosecution.
4. Unauthorised copying of information belonging to others is unacceptable.
5. Users are responsible for the security of their own work. Students are expected to back up their work. Providing a paper or electronic copy of your work to other students to gain or confer unfair advantage is deemed to be unethical.
6. Any attempt to interfere with the normal operation of the College's ICT network OR subvert security measures in unacceptable.
7. Any use of the ICT network to send or record messages which are inconsistent with the ethos of Investigator College is unacceptable.
8. It is the users responsibility to report to a member of staff:
    a. any action which you consider may contravene the ethics of computer use; or

b. any malfunction of equipment so that repairs may be affected immediately.

Policy on Student use of the Internet [all devices]

In educating and equipping our College community to live and work in a rapidly changing world the College believes it is important to learn how to use available technology in a responsible manner.

As the internet provides connections to a multitude of other computer systems around the world, and as it is impossible to guarantee close supervision at all times, users and supervisors must understand that the College cannot control the content of information accessed. It is possible that users may inadvertently come across material on the internet which is not in accordance with the College's or your family's values.

How students will use the internet

Students will be searching for information on set projects on the internet in class time, and out of class time they will be able to undertake their own research projects.

Level of student access

There is a wireless network throughout both the Victor Harbor and Goolwa Campuses of Investigator College providing internet access via students' log on passwords. Where students have access to email, they are expected to adhere to College guidelines for email etiquette.

User responsibilities

Use of the internet at Investigator College is a privilege, not a right. Inappropriate use may result in loss of user privileges. As always, students are to take full responsibility for their actions and their effect on the College community. The College is not responsible for any loss or corruption of data (resulting in loss of grades etc).

It is the student's responsibility:

- To check for himself/herself the integrity of information taken from the internet
- To adhere to copyright law by not copying and/or redistributing another's work or property
- Not to log on in someone else's name
- Not to copy the ideas of others and not to present it as their own
- To leave any College devices set up as they find them
- Not to load any application programs or files to College hardware
- To report any malfunction in equipment to a staff member immediately
- Not to seek out or create material that could be offensive or defamatory to anyone; this includes information that could be deemed to be racist, sexist, pornographic, irreligious or contains abusive language
- Not to disclose personal details in any conversation

Students are to complete a Student Internet Agreement, sign it and have it countersigned by a parent/caregiver.

ICT Network Users Contract

All users of the College ICT infrastructure and internet agree to the following conditions of use:

Ethical Use

I agree that:

1. I shall not place software or other files on the College network where these may lead to damage or legal charges. This particularly refers to destructive programs such as viruses and pirated software.
2. I shall not use the ICT network to make unauthorised copies of copyright, licensed or patented material.
3. I shall not use the ICT network to defraud or to create false or misleading information.
4. I shall not act as though I intend to break the law by, for instance, attempting to guess a password or gain unauthorised access to any other devices.
5. I shall not attempt to monitor or read files or communications of other users.

Cooperation and Appropriate Use

I agree that:

1. I shall not waste computer resources [e.g. unnecessary printing or unnecessary time on the internet] or disadvantage others by monopolising equipment.
2. I will only attempt to send or record messages which are consistent with the ethos of Investigator College.
3. I shall not damage, hide or alter facilities, information or files.
4. I shall not interfere with the legitimate use of the facilities, networks or software products.
5. I shall keep the facilities clean, tidy and free of hazards.

Access to Computers and Devices

I agree that:

1. I shall not alter anything on any of the systems throughout the College [i.e. system files, system configuration, folders or other technical data]. If I need access then I shall see a member of the College ICT staff.
2. I shall leave all devices set up as I found them and leave the workstation tidy.
3. I shall not consume food or drink within proximity to any College device.
4. I shall not disclose my password or that of any other person and I shall take precautions to prevent unauthorised access.

CYBER SAFETY

YEAR LEVEL	SUBJECT(S)	THEMES	CONTEXT
REC	ICT	How to search the internet	Students are highly supervised and use a shared log- in and maximum level screening. The cyber-safety element is covered via student-teacher discussions and instructions.
1	ICT	How to search the internet	Students are highly supervised and use a shared log- in and maximum level screening. The cyber-safety element is covered via student-teacher discussions and instructions.
2	ICT	How to search the internet	Students are highly supervised and use a shared log- in and maximum level screening. The cyber-safety element is covered via student-teacher discussions and instructions.
3	ICT	Responsible Internet Use	College ICT policy and Agreement Class discussions and Investigations
4	ICT	Responsible Internet Use	College ICT policy and Agreement Class discussions and Investigations
5	ICT "You Can Do It" Health/PE	Cybersafety- chat rooms, social media, email, internet searches, internet identity	http://www.cybersmart.gov.au/ College ICT policy and Agreement Class discussions and Investigations
6	ICT "You Can Do It" Health/PE	Cybersafety- chat rooms, social media, email, internet searches, internet identity	http://www.cybersmart.gov.au/ College ICT policy and Agreement Class discussions and Investigations
7	ICT "You Can Do It" Health/PE	What is cyber bullying? How to stay safe on the net? What are chat rooms? Proprietary use of phones / technology	Students and staff discuss the issues (left) with a particular emphasis on ethical use, rather than penalties for misuse. In

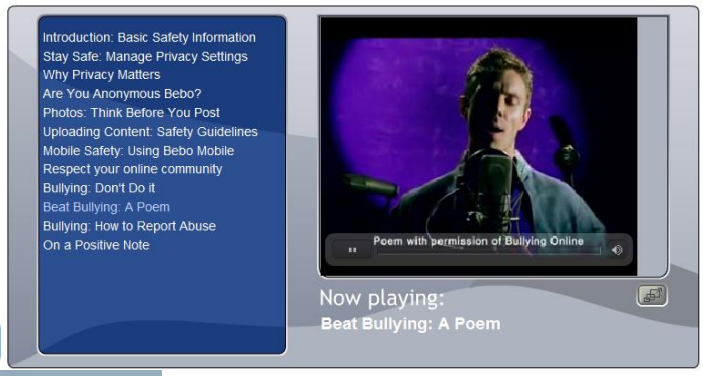
			addition to YCDI and http://www.cybersmart.gov.au/, students also access various work units via the College's "ClickView" library.
8	ICT "You Can Do It" Health/PE Christian Ed	Laws regarding internet use/abuse. Social media- responsible use Mobile phones- appropriate use (snapchat etc)	Students and staff discuss the issues (left) with a particular emphasis on ethical use, rather than penalties for misuse. In addition to YCDI and http://www.cybersmart.gov.au/, students also access various work units via the College's "ClickView" library.
9	ICT Christian Education		
10	ICT Christian Education		
11	Research Project YCDI Senior School and SACE Information	Intellectual property Saving and acknowledging work Identification of valid sites and information Laws of defamation and libel Parties and safe-partying Scams and phishing	Guest Speakers including SAPOL, University Representatives, http://www.cybersmart.gov.au/, Other College-endorsed on-line sources(see below)
12	Senior School and SACE Information	Pre-schoolies information Privacy Act Plagiarism and Intellectual Property Valid websites and Information Parties and Safe partying Safeguarding virtual identity Credit Cards and on-line purchases On-line enrolments/subscriptions	Guest Speakers including SAPOL, University Representatives, http://www.cybersmart.gov.au/, Other College-endorsed on-line sources(see below)
COLLEGE COMMUNITY		Parental supervision and help Agencies for assistance Screen time guidelines Homework Social Media Parties and Invitations Mobile phone guidelines Privacy Email contact	AFP Document: Protecting your on-line reputation http://www.cybersmart.gov.au/, Parenting Ideas (Michael Gross) Parent Information Sessions (e.g. MS and SS) Website Information for parents (see below) College ICT Policy Parenting Ideas College Newsletter

ON-LINE RESOURCES ENDORSED

AND UTILISED BY THE COLLEGE

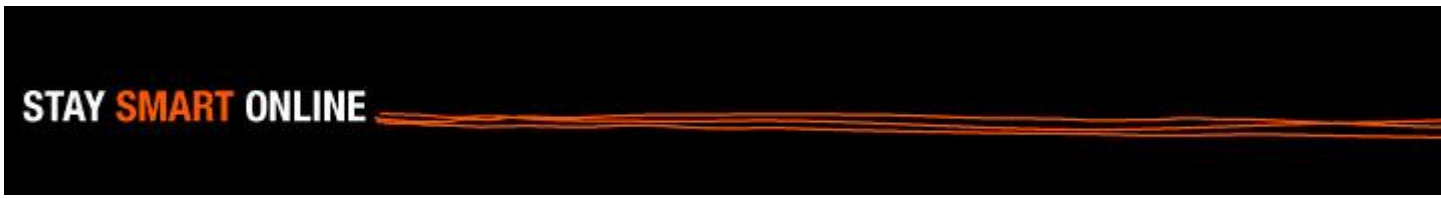
cybersafety help

acma



cyber(smart:)

THINK U KNOW .org.au



Rules Specific to Yammer

Principles

The College Network and ICT Facilities are for ACADEMIC, PASTORAL and ADMINISTRATIVE use only. They are not intended for SOCIAL, FRIVOLOUS or VEXATIOUS purposes. Like the College Diary, ICT devices and networks provide staff, parents and students with an open, formal and accessible means of communication.

Students (or staff) who use the College Network and ICT Facilities for uses other than the above are effectively misusing these facilities. Indeed, they may well be depriving other users of valuable bandwidth, as well as potentially causing system failures and faults due to unauthorised and/or inappropriate use. Inappropriate use wastes the time of ICT staff, teaching staff and students in addition to creating an unproductive, inefficient and unsafe on-line learning environment.

Important new Rules

In the case of any College Network application, including Yammer and Email:

1. All groups are made by teachers and must have a teacher in them to moderate content. Groups created by students will be deleted. Groups with no teacher will be deleted.
2. Students must only join groups appropriate to their year level
3. Students must leave their display name as their full name and use an appropriate profile picture. Change of profile name to something unrecognizable or profile picture will result in account and all content posted by that user being deleted without warning.
4. Discussion is for school related use only.
5. Students receive one warning for inappropriate use from teacher, Head of School, or ICT staff. Such warnings MUST be logged on Synergetic as evidence.
6. Students who do not respond to a warning will be deleted and banned from Yammer/Email etc for remainder of Term/Year and noted in student record 'CommsLog' as per normal discipline procedure
7. Misuse deemed severe and/or criminal will result in IMMEDIATE suspension of ICT privileges.

Mobile Phones/Devices [BYOD - Bring Your Own Device]

The College recognises that mobile devices [phones, smart phones, tablets etc.] are a valid and important communication tool and a part of contemporary society. At Investigator College we believe that it is in everyone's interest to limit student's use of mobile technology because of the nature of the College's environment and because of the risk of loss or damage. The College also recognises that students will use mobile technology in particular circumstances but this needs to be managed effectively through policy, procedure and an education process of the etiquette surrounding their use in society.

Due to the College's duty of care responsibility for each student it is expected that all external communication between students and parents during College hours is conducted by [or with the knowledge of] the College through Student Services.

Principles

Investigator College aims to create and sustain quality learning environments that will not be compromised by mobile phones. General principles that underpin any mobile phone use at the College include:

1. Mobile phones will be used responsibly by students in accordance with requirements of civil and criminal law.
2. Mobile phones will not intrude on the learning environment.
3. Mobile phones will not violate the integrity of assessments and therefore will not be allowed into tests and/or examination centres.
4. Students who bring mobile phones to school agree to proper usage patterns and accept liability for replacement in the event of theft or damage.

Mobile Device Photography and Video

1. Mobile phones should not be used for taking photographs, voice recording or video footage of persons in or around the College or at any College function or activity unless it is for an expressed, legitimate and approved College function or activity for which prior permission has been sought and given, both from the College and from the individual being photographed, filmed or recorded.
2. Any material gathered through such a process must only be used for that permitted purpose.
3. Photographs, voice recordings and video footage of any kind may not, under any circumstances, be emailed, posted or loaded onto any website, published or otherwise distributed in any way other than in strict accordance with the above.
4. Failure to observe these rules may constitute a serious breach of others' privacy, for which there may be civil and /or criminal legal consequences.

Implementation

1. The College does not accept responsibility for lost or damaged student mobile phones.
2. Mobile phones and students using them must not cause disruption to classes or individuals.
3. If a student brings a mobile phone to school it is to be turned off and out of sight in classes, meetings, assemblies or similar organised activities. The only exception to this is when a teacher has given explicit permission for a mobile phone to be used in a learning task (e.g. to take a photograph).
4. Students misusing mobile phones at school will be brought to the attention of the relevant Head of School.

5. The College reserves the right to prohibit students from bringing mobile phones into certain spaces or during certain activities e.g. exam rooms.

Management Protocol

Students misusing mobile phones at school will have their phone confiscated.

a. The phone should be placed in a manila envelope and labelled with the student's Name, Home Group and Date.
b. The phone should be handed to Students Services.
c. An email should sent to the student's Home Group teacher/HOS.
d. The student can redeem the phone at the end of the day – HOS/Home Group teacher may impose an additional penalty.
e. In the case of repeat offenders, the Head of School may insist that a parent of the student redeems the phone.