FRASER COAST
ANGLICAN COLLEGE

CYBER SAFETY AND SOCIAL MEDIA POLICY

Enriching Body, Mind & Spirit

Important terms used in this document:

(a) The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies.

(b) 'Cyber safety' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones

(c) 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below

(d) The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), 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 mobile phones, video and audio players/receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.

Rationale

Fraser Coast Anglican College has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the school community.

These responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school. A policy currently exists for staff and student's use of ICT; this policy will deal with cyber safety issues and will include strategies for the College, Parents and Students to use to eliminate or minimise the potential of illegal cyber activities.

Fraser Coast Anglican College places a high priority on providing Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the College recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The College thus acknowledges the need to have in place rigorous and effective school cyber safety practices which are directed and guided by this cyber safety policy.

Policy

Fraser Coast Anglican College will develop and maintain rigorous and effective cyber safety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

These cyber safety practices will aim to not only maintain a "cyber safe" 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.

Policy Guidelines

Associated issues the school will address include: the need for on-going funding for cyber safety practices through inclusion in the annual budget, the review of the school's annual and strategic plan, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cyber safety for the school community, disciplinary responses appropriate to breaches of cyber safety, the availability of appropriate pastoral support, and potential employment issues.

To develop a cyber-safe school environment, by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. These will be based on the latest information, best practices and procedures available at the time.

A process for reporting back to the Principal will be agreed upon and established. Frequency and content of reporting will be included.

In recognition of its guardianship and governance role in the cyber safety of the school, the Council will also develop a policy relating to Councillors' use of ICT devices / equipment. This will cover all use of school-owned/leased and privately owned/leased ICT devices/equipment containing school data/information on or off the school site

Guidelines for Fraser Coast Anglican College Cyber Safety Practices

1. The school's cyber safety practices are based upon information contained within relevant government, diocesan or other relevant best practice for Australian schools.

2. 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/leased 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.

3. Fraser Coast Anglican College use agreements will cover all the college community, and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.

4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.

5. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Fraser Coast Anglican College is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.

6. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.

7. 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.

8. The school has the right to audit at any time 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.

9. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of Privacy legislation current at the time.

10. The safety of children is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cyber safety practices. In serious incidents, advice will be sought from appropriate sources. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Information for Students

To be good cybercitizens everyone who has the ability to access, understand and participate in or create content using digital media should know and use some basic rules.

If you publish anything to the web it will remain there forever;

Do not publish any personal details;

Project an appropriate image – employers trawl through social sites as part of their interview process;

If you want to post information, images or videos of other people – get their permission first; and,

Make sure that you reference any information that is not yours and acknowledge where it came from.

Downloading of information needs to be done safely and ethically:

Only download from reputable and/or trusted sites or people (including emails and instant messages);

Make sure that you read the terms and conditions and that you understand them – ASK if you are not sure;

Use the content appropriately and as it was intended to be used;

Make sure that you check any copyright issues; and,

Check the size of the file being downloaded – exceeding data limits may cost money or slow up your system. Downloading to a mobile phone from the internet can leave you with big bills at the end of the month.

Positive online behaviour is the ability to develop positive, appropriate and constructive online relationships with peers, family and strangers in a variety of mediums; this includes:

Making sure that all communication is respectful;

Making sure that emoticons are used when making a joke or being sarcastic;

Being able to react appropriately when offensive or hurtful communication is received; and,

Developing and updating your skills for positive communications between yourself and other people online.

Cyberbullying is a text-based way of bullying someone and can be received by:

Mobile phone;

MSN Messenger;

Chat rooms;

Social Networking Sites;

In-site chat areas; or,

Email

It is important to know how you can try and prevent cyberbullying or what to do if it happens to you:

Cyberbullying is NOT okay – tell someone you trust;

DO NOT ERASE THE TEXT OR EMAIL

Use the Cyber safety help button on the Cyber smart website;

Remember to keep your passwords secret;

Remember to keep mobile phone numbers private – only give your number to someone you trust;

Do NOT reply to nasty messages and/or block the sender if they are in your contact list;

Call the Cyber safety Contact Centre on **1800 880 176**; and,

Report the sender to the messaging or email service provider.

Accessing social networking sites can have many benefits; however, there are potential down sides as well. You need to take care of your own and other people's identities and personal information.

Protect your privacy and personal information;

Set your sites to private

Only allow friends you know in real life to have full access to your profiles

Have appropriate contacts;

Do not allow strangers into your private networks

Avoid inappropriate content;

Avoid flirty or suggestive names

Do NOT post flirty or suggestive photos or other images

Sexting is the sending of sexually explicit images by mobile phone.

Sexting can have serious consequences for the person sending the image AND the person receiving the image;

NEVER post or distribute sexually explicit images of yourself or others;

If you receive a photo – speak to a trusted adult about it;

There is a real potential for predatory sexual behaviour;

Everything you do leaves a digital footprint – it never goes away;

Follow appropriate guidelines for internet and mobile phone use.

e-Security is available and should be used to protect you when you are online. Your personal information can be stolen and used for many things, most of which are illegal. The misuse of personal information can lead to financial loss and other people using your identity.

To help combat the risks you should:

Use up-to-date anti-virus technology – worms, Trojans, viruses or other malware can infect a computer and have the potential to steal information, send spam and destroy files;

Keep any anti-virus technology up to date – you may need to do this once per hour on broadband connections;

Use good security practices to minimise the risks of infection;

Use a Firewall to prevent or limit unauthorised access;

A firewall can be part of an external device, software based or a standalone device.

IF YOU RECEIVE NASTY EMAILS, TEXTS OR ARE SUBJECTED TO ANY OTHER SIMILAR CYBERBULLYING ACTIVITIES – TELL A TRUSTED ADULT

IF IN DOUBT TELL YOUR TEACHER

Information for Parents

Children and young people are growing up with the internet and technology as part of their everyday life.
They use it:
For school work, whether that is at home, on the bus or at the College for assignments, homework or research;
As a source of information and/or entertainment;
As a key communication tool; and,
As a very important means of socialising with their friends, strangers or mentors

With greater use of the internet, faster speeds and the availability of information, people are now able to:
Easily contribute text and multimedia to online sites;
Share content among users; and,
Have live text-based conversations or VOIP (Voice over Internet Protocol) facilities.

Generally, the older the child the more they will use technology and consequently be on the internet for longer periods. Access and use of technology is seen as a part of 'fitting-in' as a teenager with pressure from their peers being enormous. The use of technology is seen as being a very important part of maintaining social currency.

Many of the sites that children or young people are using will be blocked by systems within the school; however, there may be little or no restrictions on these sites when at home. It is an important that both the College and parents be familiar with the technology that the students are using and the sites that are being accessed.

Information is constantly being given to students and also being reinforced within various subjects as to how they can be a good "cybercitizen". As a parent it is important that you understand the basis of this information flow and the areas or capabilities that a good cybercitizen's profile is based upon:

1. Digital Media Literacy – the ability to access, understand and participate in or create content using digital media, including
    a. Critical Literacy;
    b. Publishing safely and ethically; and,
    c. Downloading safely and ethically.
2. Positive online behaviour – the ability to develop positive, appropriate and constructive online relationships with peers, family and strangers in a variety of mediums. This may include:
    a. Appropriate on-line contact and communication with others
    b. Consideration of issues such as cyberbullying, problematic usage or unethical behaviour
3. Peer and personal safety – the need to develop protective behaviours while using a range of online media including social networking sites. In addition, students must have the need to care for themselves and other people's identities and personal information. Consideration should be given to:
    a. Protecting personal information and privacy – for example: setting social networking sites to private; only allowing friends you know in real life to have access to profiles; avoiding flirty or suggestive names; not posting flirty or suggestive photos or other images; and, not allowing strangers into private networks.
    b. Appropriate contact – making sure that the person "chatting" is who they say they are; friends of friends may not be known to anyone; and, sites are available where "friends" can be hired by the hour, which has the potential to allow complete strangers into the group.
    c. Avoiding inappropriate content – Sexting is the sending of sexually explicit images via mobile phones and is a widespread issue with potentially serious consequences for both the sender and the recipient. Images of young children may be deemed as child pornography with potential legal consequences. Students do not necessarily realise that once a photo has been sent it cannot be retrieved; this can lead to humiliation, cyberbullying or even sexual assault. Images can be uploaded to the internet and be across the world in minutes; photos can be forwarded to multiple mobile phones instantly and forever; once an image is on the internet it will stay there forever.
4. E-Security – the use of hardware and/or software as well as online security to combat malware, viruses, trojans or other malicious code from entering the computer or protecting an individual. The ability to understand how personal information can be compromised; the identification of security risks when downloading and sharing information; and, the identification of ways to protect computers. Malware can be prevented by:

    a. Using anti-virus technology – viruses, trojans, worms and other malware can infect a computer with the ability to steal information; send spam; or, destroy files.
        i. It is essential that anti-virus technology be kept up to date and this can mean as much as once per hour on a broadband connection.
        ii. The use of good security practices can minimise the risks of infection.
    b. Firewall technology – can prevent or minimise unauthorised connections to and from the internet.
        i. A firewall can be part of an external device such as a router; it can be a dedicated device; or, it can be software installed onto the computer.
        ii. A firewall can also provide mentoring of network activity.

There are legal implications of using technology in schools in that the college has an obligation to eliminate or minimise the risk of harm to students. To meet these obligations, the College has systems in place on the student and staff intranet to prevent access to inappropriate content, inappropriate sites and to prevent bad cyber citizenship.

Where students have access to a mobile phone within the college, there is a high potential that they can access any part of the internet without any restriction. It is essential that the messages that are being taught within the College about good cyber citizenship be reinforced outside the school environment.

Policies and procedures exist within the College to help manage the risk, protect users, protect the organisation and to keep the issue of cyber safety as an integral part of any planning or activity.

Information for Teachers

It is essential that a whole of College approach is made to Cyber safety so that staff and students know what is and is not acceptable. Some of the ways that this can be achieved are by:

- Establishing a cyber-safety team (committee) – can greatly assist the implementation of a holistic approach to cyber safety within the College. The cyber safety team can also assist students to understand and manage appropriate use of personal information. In addition the cyber safety team can lead the management of issues within the College, audit policies and procedures as well as providing for the establishment and embodiment of new college-wide cyber safety behaviours.
- Establishing cyber safety contact person(s) – someone to whom staff, students or parents can go to for advice on cyber safety issues; to report inappropriate behaviour or cyberbullying; and, to promote cyber safety and good cyber citizenship within the College Community.
- Developing appropriate policies and procedures – practical policies with simple rules to promote good cybercitizens that may include appropriate inline behaviour; clear consequences of hostile online behaviour; methods for redressing inappropriate behaviour; bystander reporting rules; and, the provision of clear reporting and support mechanisms for those involved.
- Educating students, parents and staff – Cyberbullying, for example, poses unique challenges to all three groups of people with the impact on one individual also affecting many others. Places that were once associated with safety can now be easily intruded upon by the use of mobile phones or the internet. It is important to educate students, staff and parents so that they can identify good or bad cyber activity.

Common Cyber safety issues include Cyberbullying; Unwanted Contact; e-Security; the protection of personal information; accessing inappropriate content or excessive internet use.

Cyberbullying – the use of different electronic media to send abusive texts or emails; taking and sharing unflattering or private images (including naked or sexually explicit); posting unkind messages or inappropriate images on a social networking site; the exclusion of individuals from online chats or other communication; the assumption of another person's identity online and representing them in a negative relationship with others; and, repeatedly (and for no apparent strategic reason) attacking players in online gaming. Whilst cyberbullying is similar to 'normal' or real-life bullying, there are some notable differences. For example, it can be difficult to escape and it is invasive; it can occur 24 hours a day and 7 days a week; the victim can be targeted at home; harmful material can be widely and rapidly disseminated; a large number of people can receive information or images immediately and be anywhere worldwide; the actual bully may have a sense of relative anonymity and be some distance from the victim; and, there is no immediate feedback or consequence to the bully.

Unwanted Contact – electronic media such as the internet allows individuals to learn, communicate, research and socialise with other people anywhere in the world. Although research and the ability to learn are valid and popular uses of the internet, many young people find the appeal of communicating and socialising with existing or new friends a higher priority. Virtual worlds, social networking, content creation, chat rooms, online gaming and other similar sites allow young people with shared interests to come together online regardless of their location. Children or young people can have 'friends' or friends-of-friends introduced to them within the various sites, which allows for a wide variety of views and ideas. The potential is that not everyone on the internet behaves in an ethical or responsible manner. Individuals can be deceptive about their true identity and can use this to communicate with young people in chat rooms; lead discussions about inappropriate topics; misrepresent individuals for malicious purposes, including cyberbullying; and, groom young people for the purposes of unlawful sexual activity. It is essential that students be educated to only communicate with persons that they know and trust in real life.

e-Security – There are many ways in which computers can be "attacked", some of these include adware, malware, scams and fraud; spyware; trojans; Viruses; and, worms. Each of these intruders can be downloaded from the internet inside or attached to files such as images, music or other documents. Any one of these intruders can affect personal information; the computer itself; or, can be sent to computers of friends to do the same thing.

Protecting Personal Information – personal information is stored on individual computers or mobile phones and is also used to access various areas of the internet. Online purchasing; joining websites; entering competitions; and, online gaming or virtual worlds all require personal information to be given prior to entry. Names, addresses, phone numbers, dates of birth etc may be requested upon registration or as part of the security system allowing later access.

Inappropriate content – is that which breaches the norms or usual applicable standards on social, religious, cultural or other grounds and may include violent content; sexually explicit material; extremism; hate or vilification; the promotion of crime or violence; or, online advertising.

Excessive Internet Use – it is difficult to quantify how long an individual should spend online; however, where warning signs or symptoms are displayed, safe limits may have already been breached. Students studying for an assignment may spend a great deal of time researching a topic or writing a report; however, there is a greater potential for young people locked into gaming sites or social networking sites to be on the internet for long periods. Changes in behaviour or physical indicators may identify excessive internet use and may be identified by showing a general decline in a student's health or well-being; constant talk about particular online programs or games; appearing anxious, depressed or irritable; showing signs of isolation or becoming withdrawn; declining academic standards; information from parents or siblings about internet usage; or, reports of many late nights.

The College has an obligation to maintain the health, safety and welfare of its staff, students and any other persons who visit the site. An obligation also extends to the protection from harm of students whilst in the College and when on authorised excursions or other activities away from site.

Students are told that they should go to a trusted adult if they are confronted by cyberbullying – that could be you! There are things that you can do to help eliminate cyberbullying from the College; consider the following:

- Ensure the student is safe and arrange appropriate support;
- Continue to give support whilst the incident is being dealt with;
- Contact the student's parents to alert them of the issue;
- Meet with the parents to discuss strategies;
- Reassure the parents and student that the College is taking the matter seriously;
- Gather basic facts and, if possible, identify the students involved;
- Implement appropriate procedures to address the bullying using evidence-based responses such as restorative justice approaches to conflict resolution. These approaches seek to address bullying issues while providing support to both the victim and the bully. This approach can be used to strengthen the school community and respect individuals.
    - Examples of evidence-based approaches to address bullying are provided at Bullying. No Way!
    - Additional information can also be located at: www.bullyingnoway.com.au/

There is a potential that you, as a teacher, may have access to and use social networking sites to keep in touch with friends or family. Students or parents of students may wish to become one of your "friends" within the site, especially if you are involved in clubs or sports teams etc. together. Things that you may say to your family and friends can be accessed by anyone that you give "friendship" to; this could leave you open to all sorts of conflicts or problems.

Social Media

College Responsibilities-

Fraser Coast Anglican College take a shared responsibility with parents in identifying and addressing issues relating to social media. The college will educate the students of their social media responsibilities as part of the enrolment process and as well as during their pastoral program.

Parent Responsibilities-

Parents play a crucial role in helping their children enjoy safe and positive experiences online. The college encourages parents to be aware of risks faced by their children and to employ strategies to manage these risks. Parents who want to report inappropriate use of social media involving their child or the college are encouraged to obtain hard copies of the relevant material e.g. printouts or screen shots.

Student Responsibilities-

All students are directly responsible for any content they post on social media sites. Social media is currently not used as part of the academic or pastoral program here at the college and therefore its use here at the college by students is considered inappropriate. Therefore:

1. Students are not permitted to use social media while at school.

2. Students are not permitted to upload any media to social media sites that portrays an association with the college. This includes but not limited to, photos or video of students wearing uniform, photos or video of students or staff within the college grounds, audio of students discussing the college.

3. Students are not permitted to post comments on social media sites that specifically name the college, members of its staff or groups of its wider community (P & F, Fraser Flames, College Foundation), in a negative context.

4. Students are not permitted to post comments or media on social media sites about other students (from any educational institutions) that are derogative or offensive in any way.

Students who want to report inappropriate use of social media involving themselves, other students or the college are encouraged to obtain hard copies of the relevant material.

Possible Consequences for Breach of Student Responsibilities

The college is legally entitled to control the use of social media within its grounds and defend itself against defamatory material posted online. Students who have breached their social media responsibilities could face the following consequences.

1. Students accessing social media at school via computers, breaches the college's "Student Acceptable Use of College Computers and Network Policy", and are in breach of their student agreement and therefore face consequences as per the policy (page 2). Accessing social media via mobile device (even if the device is not sighted by a staff member) is in breach of the college's" Mobile Phone Policy" and the phone will be confiscated for 3 school days, (as per the Mobile Phone Policy).

2. Students who have uploaded media to social media sites that portray an association with the college are required to remove them immediately. The college reserves the legal right to directly contact the social media organisation and advise that the student has breached that organisation's "Statements of Rights and Responsibilities" in regards to intellectual property. Depending on the situation, the college reserves the right to take further punitive or legal action at the discretion of the Principal.

3. If the college becomes aware of incidences that occurred on school grounds through social media, then action will be taken in line with the particular sub schools "Behaviour Management / Bullying Policy".

4. Cyber bullying or other inappropriate online behaviour involving other students that occurs outside and independent of the college will be regarded as an "out of school incident", and is not subject to any of the college's behaviour management policies. The college does, however, feel a duty of care for its students that goes beyond any legal framework and in such cases where it be aware of serious incidents will endeavour to contact parents of all students involved and /or the police(where appropriate), to inform them of incidences involving students.

Marketing

Aim-

Fraser Coast Anglican College aims to use social media to meet its goal of the marketing plan, which is to "*develop an extensive communication plan that allows the college to communicate effectively both internally and externally.*"
The college recognises that a significant proportion of its parents and students use social media frequently and that social media can be used as a marketing tool to promote the college at a low expense.

Authorised Use-

Only authorised users will be allowed to make posts on the Facebook page. Staff authorised to add posts to the college's Facebook page are;

- The Executive Leadership Team (ELT)
- Page Administrator (as designated by the principal)
- Marketing PR Officer
- Directors
- Any other person so authorised by the principal

Fraser Coast Anglican College will have its own Facebook account and the password will be shared with authorised users only. Authorised users are obliged, under no circumstances, to share their password with any unauthorised person.

Information for Authorised Users

Protocols for posting content-

Authorised staff are encouraged to post comments relating to;

- The promotion of significant upcoming events related to their area.
- Significant achievements / participations by staff, students and programs within their area.
- Intellectual discussion on academic curriculum / pastoral issues related to their department's academic or pastoral program.
- Thanking people for significant contributions to the college or related events.

All comments, wherever possible, should be accompanied by a link that redirects the user back to the college's website, newsletter or other relevant credible site.

Guidelines for posting comments-

- Staff should use formal language at all times, (similar to what is required for reporting).
- When mentioning a student their full name should not be used. Use first name and initial for surname.
- Spelling, punctuation and grammar must be correct.
- Staff should not post comments about frivolous matters such as homework or assignment reminders, weekly sports score or general staff notices.
- Comments should not be reposted or recycled.
- Comments should not be used to promote events that are not directly related to the college's operations, such as personal causes, charities or parent businesses.
- Controversial or divisive topics and opinions should be avoided.
- Any comments relating to religious matters should be restricted to reporting on student involvement or achievements rather than expressing options on doctrine.
- All authorised users should accept there should be a balance of posts from across the school and that one department or area should not appear to dominate the posts.

Authorised users who feel that a posting by another user does not meet the guidelines, should immediately remove the post. If you have to action this for any reason please let the person know who posted it, so they can repost the comment once the necessary changes have been made.

Media-

Authorised users are encouraged to post media. Examples of appropriate media could include photos or video of school work, the college facilities or grounds and distant / obscured groups of students where individuals or their names cannot be clearly identified. Images must not be "tagged".

Promotional material that is already in the public domain, (such as TV / radio advertisements, newspaper articles etc.), are acceptable, but should be removed if a parent or student objects.

Photos or video of parents and staff can be posted if they have given their permission once they have seen and approved what is to be posted. This approval should be via email so a copy can be recorded.

Events-

Authorised users can use the "EVENT" application to promote a significant[1] upcoming event. Less formal and more frequent posting is acceptable within the event's own discussion board.

The "EVENT" app should not be used for in-school student organised events, such as fundraising night and free dress days.

[1] Significant event may include; P & F events, Musical events or sub school events such as Middle School meander.