Staff e-Safety/ Social Networking Policy

The safety and protection of our students is paramount. The Head and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

As such, this policy is an integral part of our Safeguarding provision. It is intended for St George Catholic VA College staff and is designed to protect the interests of staff and their families as well as students and their families. It applies to those who have access to and are users of school ICT systems, both within and outside of the school. It sits alongside, and supports, the Student Computer Use Policy and Agreement, which all students of the college must read and sign.

RESPONSIBILITY AND ACCOUNTABILITY

Headteacher/ Senior Leadership Team:

- Should ensure that all existing and new staff are familiar with this policy and its relationship to the School's standards, policies and guidance on the use of ICT.
- Should provide opportunities to discuss appropriate social networking use by staff on a regular basis, and ensure that any queries raised are resolved swiftly
- Must ensure that any allegations raised in respect of access to social networking sites are investigated promptly and appropriately, in accordance with the School's Disciplinary Procedures and Code of Conduct and Disciplinary Rules.

Employees:

- Should ensure that they are familiar with the contents of this policy and its relationship to the School's standards, policies and guidance on the use of ICT
- Should raise any queries or areas of concern they have relating to the use of social networking sites and interpretation of this Policy, with their line manager in the first instance.
- Must comply with this policy where specific activities/conduct are prohibited.

Governors:

- Will review this policy and its application on an annual basis
- Should ensure that their own conduct is in line with that expected of staff, as outlined in this policy.

AUTHORISING ACCESS

All staff must read and sign the 'Staff e-Safety and Social Networking Policy' before using any college ICT resource. The college will maintain a current record of all staff and students who are granted access to college ICT systems.

Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement. Parents/carers will be asked to sign and return a consent form.

Staff must not allow students to use their computer when logged in under staff user name.

SOCIAL NETWORKING

Social networks are rapidly growing in popularity and use by all ages in society. The most popular social networks are web-based, commercial, and not purposely designed for educational use. They include sites like Facebook, Twitter, Instagram, Reddit, Pinterest, MySpace, Bebo, and Xanga. For individuals, social networking sites provide tremendous potential opportunities for staying in touch with friends and family.

Other educational networking sites are also growing in use. These sites are usually restricted to only certain users and not available to the general public. These include resources such as Moodle, educational wikis, professional online communities such as Classroom 2-0 Ning, or online applications such as Google Apps for Education.

As educators we have a professional image to uphold and how we conduct ourselves determine this image. There have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue about their schools and or students or posting pictures and videos of themselves engaged in inappropriate activity. Some educators feel that being online shields them from having their personal lives examined. But increasingly, educators' online identities are too often public and can cause serious repercussions.

Access:

Accessing social networking sites in working time and/or from School ICT equipment is strictly forbidden, whether the equipment is used at home or at college.

Befriending:

This policy is not intended to restrict all employee activity on social media however school representatives are asked to exercise caution and professional judgement about what they use it for, who they communicate with and subject matter. Colleagues are advised to make full use of the security settings available within the systems but note that these cannot be guaranteed to provide protection against allegations being made or disciplinary action being taken. The college considers having pupils and current parents as 'friends' on social networking sites to be problematic and something that might very easily compromise a member of staff professionally or impact upon the school's reputation. It is, therefore, the school's strong advice that staff should not have current pupils as 'friends' in this environment.

For the protection of your professional reputation and the reputation of the college, the following practices are strongly recommended:

- Do not accept students (or their siblings) as friends on personal social networking sites. This includes ex-students for at least 2 years after they leave the college (i.e. who are under 18 years old).
- Decline any student-initiate (including ex-students and siblings) friend requests.
- Do not initiate friendship with students of the college.
- Remember that people classified as “friends” have the ability to download and share your information with others
- If you wish to use networking protocols as a part of the educational process, please work with the ICT staff to identify and use a restricted, college endorsed networking platform.

Content of any interaction with students, staff or families:

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libellous.
- Exercise extreme caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
- Weigh whether a particular interaction puts your effectiveness as a teacher or member of support staff at risk.
- Post only what you want the world to see. Imagine your students, their parents your Headteacher or administrator, visiting your site or reading your mail. It is not like posting something to your web site or blog and then realizing that a story or photo should have been taken down. On a social networking site, once you post something, it may be available, even after it is removed from the site.
- Ensure that all correspondence is of an appropriate professional standard. Any email that is sent using your college address is the “property’ of the college.
- Do not discuss students or employees or publicly criticize college policies or personnel.
- Do not post images that include students.

Security:

- Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these sites are calendar programs and games.
- Run regular updates of malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
- Be careful not to fall for phishing scams that arrive via email or on your wall, providing a link for you to click, leading to a fake login page.
- Visit your profile’s security and privacy settings. At a minimum, educators should have a privacy setting set to “only friends.” “Friends of Friends” and “Networking and Friends” open your content to a large group of unknown people. Your privacy and that of your family may be a risk. People you do not know may be looking at you, your home, your children, and your grandchildren – your lives!

- Please stay informed and cautious in the use of all new networking technologies.

If you leave your laptop/computer unattended, ensure it is "locked down'.

E-MAIL

Students must immediately tell a teacher if they receive offensive email. In email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming email should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters is not permitted and limits are in place to prevent these.

PUBLISHED CONTENT/COLLEGE WEB SITE

Staff or student personal contact information will not be published. The contact details given online should be the college office. Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused.

Work or photographs can only be published with the permission of the student and parents/carers. They have the option to refuse permission when completing induction paperwork. Students are expected to inform relevant staff if their work or image is not to be published, at the time.

FILTERING

The college will work in partnership with SCC and the Internet Service Provider to ensure that systems to protect students are reviewed and improved. If staff or students discover an unsuitable site, it must be reported to their IT teacher, or the Network Manager.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

VIDEO CONFERENCING

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Students should ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing will be appropriately supervised for the students' age.

EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed. Senior staff should note that

technologies such as mobile phones with alternative access to the internet, can bypass college filtering systems and present a new route to undesirable material and communications.

Mobile phones will not normally be used during lessons or formal college time (unless the particular lesson or aspect of the curriculum requires it). The sending of abusive or inappropriate text messages is forbidden. The use by students of cameras in mobile phones to capture their own work will be kept under review. Games machines including the Sony Play Station, Microsoft Xbox and others have Internet access. Care is required in any use in college.

PROTECTING PERSONAL DATA

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

COMMUNICATING e-SAFETY

e-Safety rules will be posted in all rooms where computers are used and on the college website. Students will be informed that network and Internet use will be monitored. A programme of training in e-Safety is delivered, based on the materials from CEOP. All staff will be given the college Staff e-Safety and Social Networking Policy and have its importance explained.

MONITORING AND TRACING USAGE

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior staff and work to clear procedures for reporting issues.

Correspondence with companies, parents/guardians or outside agencies must be sent using the college email address not a personal email address.

Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

POLICY BREACHES

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy and Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal.

Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

e-SAFETY COMPLAINTS

The Headteacher or Subject Leader will deal with complaints of Internet misuse for IT. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with college safeguarding procedures.

Complaints about e-bullying must be dealt with in accordance with college anti-bullying policy.

This policy should be reviewed by the Network Manager on an annual basis to ensure the latest technological developments are included before submission to the Policy Working Group for approval.

This policy will be reviewed every year.

Date of next review: March 2018

The Policy Working Group agreed this policy on 8 March 2017.