ICT AND E-SAFETY POLICY

Last Reviewed/Updated: 01.05.2017
Next Review/Update: 01.05.2018

Policy Scope

e-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. This e-safety policy will operate in conjunction with other Regent College policies including those for Behaviour, anti-Bullying, Curriculum and Data Protection.
The policy covers the use of information technology within College premises on any devices, including:

- Use of Internet
- Use of e-mail
- Mobile phones/ smartphones
- Use of computers (desktop PC, laptop, netbook, tablet, etc.)
- Use of social networking and personal publishing
- Use of the College wi-fi
- Personal music players and any recording/storing devices

Roles and Responsibilities

Co-Principal/Vice Principal

- responsible for the safety of all children and staff
- monitor the implementation of this policy and allocate sufficient resources and training to ensure full adoption of the procedures and principles in this policy in conjunction with the network manager
- Ask parents to give consent for their children to use the Internet
- Ensure teachers guide Students toward appropriate materials on the Intranet/Internet.

Network Manager

- Use a firewall to filter and monitor access
- Monitor network usage on Watch-Guard and report quarterly to Co-Principal/Vice Principal
- Ensure virus and anti-malware protection is installed and updated regularly
- Ensure only those people with authorised access can access the College's IT network.

Staff

- Regularly discuss acceptable use with children and remind them of the College's policy and rules (this will include acceptable use of texting).
- Support parents and the community in safe use of the Internet and other technologies
- Ensure they keep data safe and secure.
- Conduct themselves professionally online; they must not allow students access to their own data through social networking sites such as Facebook; class teachers are advised to block children from their class and College.
- Inform Co-Principal/Vice-Principal of any issues of concern.

Students

- Have equal access to College-controlled email in a safe and secure environment.
- Have equal access to a variety of approved websites via the Internet.
- Be taught all the skills to use Internet and email as an ICT tool.
- Know how to report any concerns they may have.
- Use Internet and email to support, enhance and develop all aspects of the curriculum.
- Develop Internet and email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.

Internet and e-mail

Regent College provides access to internet through college devices as well as wireless network. Every student has also college email address and password which enables access to extensive suite of tools provided by Microsoft Office 365. Every student and parent is obligated to sign off "Wi-Fi Acceptable Usage Policy" before accessing College systems. Use of the e-mail address, internet and Wi-Fi is monitored by College.

Access & Security

- Access to the internet from the College's computers and network must be for educational purposes only.
- Student must not use the College's facilities or network for personal, social or non-educational use without the express, prior consent of an appropriately competent member of staff.
- Student must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the College's or any other computer system, or any information contained on such a system.
- No laptop or other mobile electronic device may be connected to the College network without the consent in writing of the IT Systems administrator.
- The College operates a BYOD wireless filtered password-protected service. Students seeking permission to use such devices in the College should sigh off the College's "Wi-Fi Acceptable Usage Policy" available from the College Support Manager.
- Students should only connect personal devices to "Regent Students" Wi-Fi network. They should not make use of 3/4G connectivity, which bypasses our filtering system.

It should be noted that traffic travelling through the College Internet connection is tracked and logged.

- Students who are not doing academic work or are creating a disruption will be asked to put the device away.
- Students should make sure they have adequate insurance for their devices including accidental damage cover that protects them in the College. The College cannot be held responsible for any damage or loss of devices.
- Passwords protect your own account within Office365 as well as the College's network and computer system. Student should not let anyone else know your passwords. If you believe that someone knows your password, you must change it immediately.
- Student should not attempt to gain unauthorised access to anyone else's computer, account or to confidential information which he is not authorised to access. If there is a problem with your password, please speak to College Support Manager.
- The College has a firewall in place to ensure the safety and security of the College's networks. You must not attempt to disable, defeat or circumvent any of the College's security facilities.
- Viruses can cause serious harm to the security of the College's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If Student suspects that an attachment sent to him, or other material which he wants to download, might contain a virus, he must speak to the teacher before opening the attachment or downloading the material.
- Student account does not have permission to disable or uninstall any anti-virus software on the College's computers.

Use of Internet

- College's computers must be used for educational purposes only.
- Students must take care to protect personal and confidential information about himself and others when using internet, even if he receives or comes across this information inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.
- Students are allowed to load material from external storage device (such as USB drives) brought in from outside only to its own dedicated student Z drive.
- Students should assume that all material on the internet is protected by copyright and you must treat such material appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work. Wherever possible, and as directed by your teachers, you should make appropriate reference in your working documents to any external sources from where you have gained copyright material for your personal use.
- Students must not bring the College into disrepute through your use of the internet.
- Students must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.
- Student will support the College approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the College or wider community.

Use of e-mail

- All students and staff have a network account and individual email addresses.
- Students must immediately tell a teacher if they receive offensive e-mails.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully in the same way as a letter written on college headed paper.
- Students must not use any personal web based e-mail accounts such as Yahoo or Hotmail through the College's network.
- College e-mail account can be accessed from home by logging into Regent Portal http://rtc.uk.net
- E-mail should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an e-mail which is not appropriate to be published generally or which you believe the Head and / or your parents would consider to be inappropriate for a Student at the College.
- Student must not send, search for or (as far as you are able) receive any e-mail message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If a student is unsure about the content of a message, speak to a member of staff. If you come across such material, you must inform a member of staff as soon as possible. Use of the e-mail system in this way is a serious breach of discipline.
- The College will take no responsibility for any offence caused by students because of downloading, viewing or forwarding inappropriate e-mails.
- Trivial messages and jokes and chain letters should not be sent or forwarded through the College's e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the College's IT system to suffer delays and / or damage.
- Students must not read anyone else's e-mails without their consent.

Published Content and the College website

- The contact details on the website should be the College address, e-mail and telephone number.
- Staff or students' personal information will not be published although pictures of students may be accessible.
- The Co-Principal and Marketing Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include students will be carefully selected.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- All parents are asked to sign a consent form, regarding photographs of students being published on the college website and other College publications, when the student joins the college.
- Students' work can only be published with the permission of the student and parents.

Social Networking

- The college will block/filter access to social networking sites. (e.g. Bebo, Facebook, chatrooms, etc.)
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Students will be encouraged to invite known friends only and deny access to others.

Photographs & Images

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Students may only use cameras or any mobile electronic device with the capability for recording and /or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- All Students must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

Use of College Wi-Fi

The College makes available Wi-Fi networks for Students and staff to use for legitimate purposes. The service is appropriately protected by sophisticated filtering services that track and monitor its usage, in line with a variety of requirements including keeping children safe in education and other safeguarding procedures, including the Prevent strategy. If users of these service choose to abuse the services, by-pass filters and such like, by whatever means, then the user will be deemed to be 'abusing' the services and the user must accept the appropriate disciplinary procedures that arise, proportionate to the severity of the 'abuse'. See **Sanctions** chapter.

Use of mobile devices

"Mobile electronic device" includes without limitation mobile phones, smartphones, tablets, laptops, MP3 players.

- Mobile phones and other mobile electronic devices must be switched off during College hours.
- Student's mobile phone should be protected by either a password or 'gesture' to prevent unauthorised access.
- Students may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Co-Principal.
- The College does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto College premises, including devices that have been confiscated.
- Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not Student is

in the care of the College at the time of such use. Appropriate disciplinary action will be taken where the College becomes aware of such use.

- The College reserves the right to confiscate a Student's mobile electronic device for a specified period if the Student is found to be in breach of this protocol. The Student may also be prevented from bringing a mobile phone into the College temporarily or permanently and at the sole discretion of the Head.
- Many Students' phones give them unlimited and unrestricted access to the internet via 3G and 4G and we ask Students to only make use of the College's Wi-Fi system for internet browsing. We are constantly monitoring the use of phones and specific advice is directed at those Students who seem/are at risk of abusing the privilege of using mobile devices whilst in College.

Sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the College Management in accordance with Regent College Behaviour Policy including, in most serious cases, exclusion. Other sanctions may include:

- Increased monitoring of Student activities
- Withdrawal of the right to access College's network, internet and e-mail.
- Unacceptable use of mobile device could lead to confiscation.

Regent College reserves the right to charge Student or his/her parents for any costs incurred to the College as a result of a breach of this policy. Any action taken will depend on the seriousness of the offence.

Regent Systems Security & Monitoring

Managing filtering, virus management & breaches

The College will monitor all content when accessing the internet via Unified Threat Management (UTM) from WatchGuard. WatchGuard is the industry's highest-performing, all-in-one network security platform, it's powerful Fireware ®operating system is the fastest, most reliable and agile platform in the industry, designed to run full versions of the leading security engines in every category.
In addition, College is in process of identifying the tools for keystroke logging. Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard. This type of monitoring will assure more preventive actions in regards to identifying potential inappropriate keywords used by students. The College aims to implement these tools by end of January 2017.

- Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Regent virus and malware filtering is controlled by Avast for Business. Avast's Dashboard allows to monitor and control virus definition updates, potential threats and notifies about any issues related to virus and malware protection.
- Inappropriate use logging by Watch-Guard connected with Active Directory produces summaries for review, which identify not only machine IP address but specific user account responsible for any suspected breach.

- Network Manager is responsible for regular reporting of breaches to Principal/Vice Principal to ensure appropriate monitoring takes place.
- Wi-Fi connectivity is divided into 3 SSIDs to cover separately students, staff and tablets;
- Our service provision for data pipeline, filtering, patch management, virus and spam filters are managed by the Assign-IT (http://www.assign-it.co.uk)
- Internally all devices are serviced by an IT Engineer who services our hardware frequently to ensure safe and appropriate use.

Legislations

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The Network Manager will maintain a current record of all staff and students who are granted access to college ICT systems.
- Access to the ICT resources and/or the internet will be withdrawn should the system be used inappropriately.

The Computer Misuse Act (1990)

- Student may not access computer material without permission, e.g. looking at someone else's files.
- Student may not access computer material without permission with intent to commit further criminal offences, e.g. hacking into the bank's computer and wanting to increase the amount in your account.
- Student may not alter computer data without permission, e.g. writing a virus to destroy someone else's data, or changing the money in an account.

Copyright law

- You are not allowed to misuse other people's creative works, such as by the copying of written, musical, or film works using computers.
- During our teaching, Students will learn how to find and use a variety of copyright free and licensed resources.
- In work Students create for exam boards, they must be very careful to quote all sources and references.

Assessing risks

- The College will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a College computer. The College will NOT accept liability for the material accessed, or any consequences of Internet access.
- The College will audit ICT use to establish that the e-safety policy is adequate and that the implementation of the e-Safety policy is effective.

Handling e-safety complaints

- The Co-Principals/Vice Principal will deal with complaints of Internet misuse.
- Any complaint about staff misuse must also be referred to the Co-Principal/Vice Principal.
- Complaints of a child protection nature must be dealt with in accordance with college child protection procedures. See Regent College Safeguarding and Child Protection Policy.
- All serious e-safety incidents will be logged in the E-Safety Incident Register.
- The Co-Principals, in consultation with the Head of Technology has responsibility for the implementation and review of this policy, in consultation with parents, Students and staff.
- The Co-Principals will consider the record of e-safety incidents and new technologies and will consider if existing security procedures are adequate.

Communication Policy

E-safety Policy & Staff

- This e-Safety policy will be stored on the network in the staff shared area with access for all staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the College e-Safety Policy in college publications and on the College website.

E-Safety Policy & Students

- Students will be informed that network and Internet use will be monitored.
- All students will sign an Acceptable Use Agreement