ST MARY'S COLLEGE CROSBY

NETWORK & INTERNET USE POLICY FOR STUDENTS

This policy is subject to ratification by the Solicitor

Contents:-

This policy applies to the Preparatory School and the College

1. College Policy

Student access to the Internet
The College encourages use by students of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our students will enter.

On-line services significantly alter the information landscape for Colleges by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials will be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the students. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by students.

Electronic information research skills are now fundamental to preparation of citizens and future employees. The College expects that staff will begin to investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will consult the Head of ICT for advice on content, training and appropriate teaching levels consistent with the College's IT program of study.

Independent student use of telecommunications and electronic information resources will only be permitted upon submission of permission and agreement forms signed by parents of students and by students themselves.

Access to on-line resources will enable students to explore thousands of libraries, databases and bulletin boards including the use of e-mail. The College believes that the benefits to students from access to information resources and increased opportunities for collaboration exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the College supports and respects each family's right to decide whether or not to apply for independent access.

The purpose of this policy is to balance the desirability of staff and pupils being able to access the vast educational potential of new technology while, at the same time, providing safeguards against risks and unauthorised material and activities.

The College's Head of ICT has prepared appropriate procedures below for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

The DSL will work with the Head of ICT and the PSHE leader to ensure a coordinated approach to whole school online safety. This includes, but is not limited to:

EPR:

Yr 7 Term 1: Online rights, responsibilities and opportunities.
Yr 7 Term 2: Online risks to mental health, danger of online grooming
Yr 7 Term 3: The similarities and differences between the online world and the physical world.

Yr 8 Term 1: Online responsibilities and rights. Different kinds of bullying – including cyber bullying
Yr 8 Term 2: The risks of online communication. What to do and where to get support to report material or manage issues online.

Yr 9 Term 2: The impact of viewing harmful online content. Distorted view of sex presented by porn/ negative impact of porn. The Law as regards sexting, long term impacts of sharing and receiving indecent images/ age of consent/ pornography. How online data is generated, collated, shared and used online.

ICT curriculum:

Year 7
- Students will understand how computer viruses are transmitted, how to recognise them and how they can reduce their risks of downloading them
- Students will understand the importance of secure passwords. They will learn a technique to help them create strong and memorable passwords to protect their school work and online privacy.
- Encourage students to think about what they post online and how they are perceived through the digital footprints they create every day of their lives.
- Understand the effects that cyberbullying can have on somebody else
- Understand what to do if they are ever cyberbullied by somebody.

think about their own behaviours online and think about the impact that they might have on someone else

Year 8 & 9
e safety and how to keep personal data safe:
- Should use different passwords and Pins for different accounts
- Users should always log off immediately after using a site where personal data has been typed in.
- Only use websites that are recommended by a trusted source e.g. teacher.
- Use a search engine that has a filter to remove inappropriate content.
- Do not open ant email attachments from a sender you do not recognise.
- Be very cautious when providing personal data.
- Be cautious about any pictures or opinions you post or send to other people.
- Do not become friends on social networking sites with people you don't know.
- Never arrange face to face meetings with a person that you meet online.
- Make sure you use the privacy control settings on all your accounts.
- Learn how to report and block any unwanted users.
- Don't use real name when using online games etc.

Cyber bullying
How to Keep safe?
Report abusive posts worst cases can face criminal prosecution.
Set strong passwords for all online accounts - mixture of letters (upper & lower case), numbers, symbols.

Sign out of accounts when not in use. If someone gets your phone etc they could gain access if you are still signed in.
Think carefully about what you post online – its there forever.

2. Roles and Responsibilities

E-safety is primarily a safeguarding issue so anyone with responsibility for the welfare of children has responsibility for ensuring that information is accessed safely. The College takes it's responsibilities under the DFE documents *'Keeping children safe in education, Sept 2020'* and *'The Prevent duty, June 2015'* seriously and this document should be referred to, along with consulting the Designated Safeguarding lead, if in any doubt. Pupils also have responsibilities and will be encouraged to develop their own sets of safe behaviours.

(a) Pupils

Responsibilities for pupils include:

- Contributing to the safety of e-safety policies
- Reading Acceptable Use Policies – and adhering to them
- Taking responsibility for keeping themselves and others safe online
- Behaving safely and responsibly to limit the risks of Internet usage
- Respecting the feelings of others
- Reporting any abuses of the Acceptable use Policy

(b) The College

The College is responsible for the effective management of safety of the Internet and for making appropriate resources available to support the development of a safe culture. Its role is delegated to the Head of ICT. Their responsibilities are to:

- develop a safety culture under the direction of their teams and to act as a point of contact on all e-safety issues
- ensure that all staff are trained in e-safety
- ensure that e-safety is embedded across the curriculum
- ensure that e-safety is promoted to parents in life outside the College
- maintain an e-safety log
- prepare reports dealing with e-safety and review any breaches of safety
- review policies and procedures on a regular basis

The ICT Staff have responsibilities, the main ones of which are:

- taking responsibility for the security of systems and data
- reporting any technical breaches to the Head of ICT
- adhering to Acceptable Use Policies

Parents also have responsibilities as follows:

- reading the Acceptable Use Policy and encouraging their children to do so discussing e-safety with their children and reinforcing appropriate behaviours at home
- liaising with the College if they suspect or have identified that their child is conducting risky online behaviour

3. College Procedures

Resource Development
In order to match electronic resources as closely as possible to the College curriculum, teachers will review and evaluate resources in order to offer "home pages" and menus of materials that are appropriate to the age range and ability of the group being taught. The Head of ICT will provide appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies. All students will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

As far as possible, the College's chosen information provider has organised information resources in ways that point students to those that have been reviewed and evaluated prior to use. Whilst students may be able to move beyond these resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferrable and may not be shared.

College Rules
The College has developed a set of guidelines for Internet use by students. These rules will be made available to all students, and kept under constant review.

All members of staff are responsible for explaining the rules and their implications. All members of staff are aware of possible misuses of on-line access and their responsibilities to all students.

4. Acceptable User Policy for Students

Students are responsible for their own good behaviour on the internet just as they are in a classroom or a College corridor. General College rules apply.

The internet is provided for students to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right, and that access requires responsibility.

Individual users of the internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with College standards and will honour the agreements they have signed.

Staff may review files and communications at any time to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disc would always be private. Computer (file) storage areas will be treated as College property.

During College, teachers will guide students toward appropriate material. Outside of College, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, films, radio and other potentially offensive media.

The following are not permitted:-

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws.
- Accessing terrorist and/or extremist material whilst on the internet in College.
- Using others' passwords.

- Trespassing in others' folders, work or files.
- Intentionally wasting limited resources.

Sanctions

1. Violations of the above rules will result in a temporary or permanent bar from Internet use.
2. Additional disciplinary action may be added in line with existing practice under the Behaviour Policy for inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

This policy will be communicated to all pupils and will be reviewed at least annually by the Head of ICT and DSL.

5. Acceptable User Policy for all users of the College network

Access to the College network will be provided for you to carry out recognised College work, but only on the understanding that you agree to follow these guidelines.

Computer (file) storage areas will be treated as College property. ICT staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect that their work and emails would always be private.

The following are not permitted:-

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws.
- Using others' passwords.
- Trespassing in others' folders, work or files.
- Intentionally wasting limited resources.
- Accessing terrorist and/or extremist material whilst on the internet in College.

- Users are responsible for good behaviour on the network just as they are in a classroom or at College. General College rules apply.

- Eating, drinking, personal grooming, and the use of aerosol sprays are not considered to be suitable activities in any classroom. Near a computer they may cause serious damage and are strictly prohibited.

- Please do not spend too long sending/receiving e-mail messages – someone else is usually waiting to use the computer. You should not waste valuable resource time sending trivial e-mails to another person in the College, or to anyone else for that matter.

- Important work files must be copied to your own removable drive in case you accidentally damage them or delete them from the network service.

- If a "virus alert" occurs when transferring work files from a removable disc please inform a member of the ICT staff immediately.

- Do not use another person's password. If doing shared work you must keep a copy of the work on your own disk in case your partner is absent from College.

- Do not reveal your password to anyone. If you think someone has learned your password then change it immediately.
- Change your password at regular intervals; at least once a term using a minimum of six characters.
- Do not trespass in others' folders, work or files.
- The unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act 1998, is not permitted.
- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.
- Programs must not be installed on a computer except by a qualified technician. Do not bring in programs on a disk or download them from the Internet.
- Games must not be loaded, played or used on any computer unless used for authorised training or teaching purposes.
- The unauthorised copying of software, contrary to the provisions of the Copyright, Design and Patents Act 1988 is not permitted.
- The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964.
- A computer should not be switched off during the College day unless it has completely locked up or is unlikely to be used again that day.
- All computers should be switched off at the end of the school day.
- Always make sure that you have completely logged off the computer before leaving it unattended.
- Please leave the computer and the surrounding areas as you find them.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on your use of the College network.
2. Additional disciplinary action may be added within line of existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

This policy will be communicated to all users and will be reviewed at least annually by the Head of ICT and Vice Principal.

Reviewed: Sept 2020 J.Thomas/N.Vagianos

Review due: Sept 2021

Appendix 1 - A PARENT'S GUIDE TO THE INTERNET

1. What is the internet?

The internet is a large number of computers all over the world, linked together with cables. In most cases, each of these computers is also linked locally to a number of other computers, in a local network. It is possible for someone using one of these computers to access information on any of the other computers. This system was established by those working in Universities and Government organisations for the fast and efficient transfer of largely text-based information around the world directly from one computer to another.

It is possible for other people, outside these local networks, to connect to the Internet by using standard telephone lines between their computers and those already connected to the Internet. A number of companies specialise in providing this service for a fee.

2. What is the World Wide Web?

To make the appearance of information available through the internet more attractive, and to assist people in finding information more easily, it is now possible for special pages and information to contain text, colours, add pictures, sound and even video. These pages, collectively, make up what is known as the World Wide Web. Most of these pages include information on the location of other pages on the World Wide Web, and it is possible to follow up links between pages with similar or related content. Moving from one page to another, regardless of where in the world they might be located, is called browsing or surfing the net or web. Many of these web pages contain information that may be useful in the classroom and it is presented in a way which is often easy to use.

A number of UK suppliers including BT and research machines, offer Schools the facility of keeping their own pages on the internet. These School "home pages" might describe a School's activities to outsiders or explain project work that students are involved in.

3. What is electronic mail (email)?

This is merely a way of sending messages from one person to another via the Internet. Each Internet user has a unique email address (such as office@stmarys.lpool.sch.uk and by sending a message to this address, the recipient can read the message the next time he/she connects to the Internet. Internet email addresses are usually provided along with College's connections to the Internet and individual students will have their own e-mail address.

4. What are the dangers of the Internet referred to in the media?

It is true that there is some material on the Internet that would be offensive to most people, and this can be accessed by children if using the Internet unsupervised. The main educational providers try to "filter" known offensive locations of material of this kind, but there is too much for this filtering to be totally effective, and the locations change frequently. The only way to block access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the Internet may be lost. It is a feature of the Internet that the information is available free. Increasing restrictions will undoubtedly lead to systems of charging for access to specific material, in addition to the other costs described. It is the policy of St Mary's College to educate students and establish an acceptable use policy and partnership between home and College in dealing with the less savoury side of Internet use.

5 Social Networking Facebook, Blogging, Twitter etc.

The use of Social Networking sites by children has become ubiquitous in society today. As well as dangers referred to above there are further issues with their use; danger of online exploitation, and a danger that thoughts which might otherwise be kept private can be shared, sometimes inadvertently with many thousands of others. Specific concerns are "trolling" i.e. a site may be taken over and abusive or threatening messages left, internet bullying, stalking, and impersonation. Parents must be aware that in misusing these sites, their children could fall foul of criminal laws; e.g. harassment, copyright regarding downloaded material (where there can be international sanctions), Adopting a false age or

gender is also an offence. There can also be civil law consequences e.g. of defamation. The College would make it clear that all its' conduct rules and policies apply equally to use of Social Networking sites whether at College or outside it, as to the Internet and indeed face to face encounters. The Acceptable Use Policy as outlined below applies as do the Colleges anti-bullying, equality etc. polices. Any behaviour which is bullying, potentially defamatory or otherwise inappropriate should be immediately brought to the attention of College staff as per the policy.

6. How can I get more information?

There are many magazines in newsagents that cater for beginners and advance users of the Internet. If you have any specific questions please contact the College and ask for the Head of ICT.