TRINITY CATHOLIC COLLEGE & SIXTH FORM
An inclusive, learning community living out Gospel values

NICHOLAS POSTGATE Catholic Academy Trust

Trinity Catholic College
E-Safety & Use of ICT Policy Executive Summary

Role and Responsibility

Every adult member of the school community who has a responsibility towards the welfare of the students has a responsibility towards keeping the students safe in their use of ICT

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Trinity Catholic College e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-safety Officer
- All digital communication with students / parents / carers should be on a professional level and ONLY carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies such as computers, mobile phones, cameras etc in lesson and other school activities where allowed.
- In lessons where Internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that may be found in Internet Searches
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Communication

Protocol

- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

School Email (Gmail)

- This is the ONLY email service that is permitted to be used to communicate with students, parents/carers or for any other official College business

Personal Email

- Under no circumstance should personal email be used to communicate with students, parents or carers. Doing so puts you at risk by using an unmonitored email system

Personal Mobile Phones

- Under no circumstance should you use your personal mobile phone for communicating with students, parents or carers by text message or voice call. Your phone number should not be given out or shared with students, parents or carers. School text message services or school mobile phones should be the only method of mobile phone-based communication
- If you have your mobile phone in school then it must be protected by either a passcode, PIN code or biometric lock. If your phone has contact details or apps which access school systems, such as email, then there is a legal responsibility to protect this data

Social Media

- Use of social media to communicate with students, parents and carers must never be conducted using personal accounts. Communication is restricted to College authorised social media accounts on Twitter and Google+ only and according to the protocol set out in the E-safety policy
- Using personal social media accounts to communicate with students (past and present) puts you in a position of incredible risk and scrutiny that has the potential to devastate your reputation and career

Use of ICT

Staff Laptops

Use

Staff laptops are only intended for use relating to College activities. While it is acknowledged that a staff laptop can be taken off site and used at home, the activities must always be appropriate, legal and inline with our professional responsibility for the welfare of children. A staff laptop must not be used for:

- Accessing Illegal / Inappropriate content
- Downloading, viewing or storing illegal content including music, films and software obtained from illegal sources such as torrents. Doing so is in direct contravention of the copyrights and patents act
- Communal use. A staff laptop may contain data relating to students or staff that needs to be protected according to the Data Protection Act

A staff laptop should spend no longer than 2 weeks (holiday periods permitting) at home without returning to school and joining the network. This is essential for the laptop to receive Windows updates and Anti-Virus updates. A laptop that has been left off-site for longer than this poses a risk to your home network and to the school network upon its return

Saving personal files and information to the laptop is not recommended. The College takes no responsibility for loss of personal electronic data and content such as music and photographs

Software

Software should not be installed on a staff laptop without first checking with the Network Manager and then only if it has been legally obtained

Monitoring

The use of staff laptops is monitored with E-Safe on-site and at home. Any behaviour viewed as inappropriate is logged and reported by the software

Desktop Machines

Use

Desktop machines are to be used with the same level of responsibility as a staff laptop. The following practices also must be observed when using a desktop PC in school

- Never leave the computer logged in and unsupervised - Alway lock the computer
- Never log off a computer without closing all programs first. More often than not, this will prevent Windows from shutting down. If the PC has then been left, the next person can cancel the shutdown and access your user profile and any open systems, including SIMS

Monitoring

All devices on the school network are filtered when accessing the Internet and unsuitable behaviour is blocked and reported. Because of the evolving nature of the Internet, it is the responsibility of every adult to report any unsuitable web content to the Network Manager to help keep the filtering systems up to date

All Windows-based PCs are monitored by E-Safe in the same way regardless of the user

Password and Data Protection

Your username and password should never be shared with anyone else. As an organisation we are responsible for sensitive data concerning a large number of people and are legally required to keep this data safe according to the Data Protection Act.
Attempting to access a computer system using someone else's credentials without explicit permission being granted is in direct contravention of the Computer Misuse Act

Monitoring and Protection Systems

Web Filter

Internet-based activity is monitored and filtered using Securly, a new breed of web-based filtering system. Users are authenticated according to their Google Apps username and password. As we are all responsible for keeping students safe, we are responsible for reporting any Internet-based issues regarding content and unsuitable websites. Web filters are reactive systems and are always one step behind as they can only block sites that exist once they are known about

E-Safe

E-Safe is installed on all Windows-Based PC's in the college. This E-Safety system monitors every action, key press and site visited on a computer and captures screen images as soon as inappropriate behaviour is detected. Once detected, the behaviour incident is sent to E-Safe, who have a forensic team analyse the incident, remove any false-positives and report genuine incidents back to school. E-safe are actively looking for

- Inappropriate/unsuitable communications
- Inappropriate/unsuitable use of the Internet
- Issues relating to child protection

- Issues relating to bullying and threatening behaviour
- Incidents relating to the Prevent Legislation surrounding terrorism and radicalisation

As the system is monitored by a forensic team trained in these issues, they do not look at incidents in isolation. They will continue to monitor for patterns of behaviour that could then indicate issues surrounding the welfare of a child or radicalisation

Legislation

We should be aware of the legislative framework under which this E-Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

There are some key areas of legislation that need to be outlined and understood relating to E-Safety and our use of ICT

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer system;
- Obtain unauthorised access to a computer system with the intent of committing further crimes;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Other important legislation stated in the E-safety policy include:

- Freedom of Information Act 2000

- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012

Declaration

I understand my responsibility for the correct use of ICT systems as an adult member of the Trinity Catholic College as set out in this document and the full E-Safety Policy

I understand the statements set out in the on-screen AUP that I accept each time I log in to the school network

- All ICT activity should be appropriate to staff professional activity or the student's education and in line with the Trinity Catholic College E-Safety Policy
- Internet access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As E-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- The usefulness and integrity of the system or its contents should not be intentionally compromised by the user.
- Use of the network or school ICT equipment to access inappropriate material such as pornographic, racist or offensive material is forbidden.

Name (printed)	Signature	Date
		/ /