ST THOMAS MORE CATHOLIC SCHOOL

POLICY ON: E-Safety

School Mission Statement: "To guide and encourage students to be responsible, caring and confident in a climate of Gospel values where they can realise their full potential and celebrate each other's success".

Introduction

This policy helps form part of the school's overall approach in relation to the safeguarding of both its staff and students. As such, this policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT Systems, both in and out of the school.

E-Safety

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Our E-Safety Principles:

1. **All staff and students will use ICT responsibly**
2. **Sound implementation of e-safety policy in both administration and curriculum areas.**
3. **The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible**
4. **The school will ensure that those individuals tasked with roles and responsibilities are effective in carrying out their duties.**

All staff and students will use ICT responsibly

Teaching and learning

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- Use of the Internet should help to raise educational standards, promote student achievement, support the professional work of staff and enhance the school's management functions

Authorising Internet access

- Parents will be asked to sign & return an Internet access consent form.
- Students will not be granted access to the internet for until the above form has been signed. This access will be controlled by the Senior Administrating Assistant for System.
- All staff must agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep an up to date record of all staff and pupils who are granted Internet access.

Safe Internet Use

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Education Walsall can accept liability for the material accessed, or any consequences of Internet access.
- The school's Internet access is filtered by the LEA to block access to inappropriate content but it must be accepted that no filtering system can be 100% effective.
- The most effective way to establish safe internet use is by educating users with regards to the potential risks involved and encouraging them to follow safe working practices.

Sound implementation of e-safety policy in both administration and curriculum areas.

Staff and the e-Safety policy

- Staff who use personal devices to access school email accounts must ensure that the device is password or pin protected.
- Staff must not use personal devices to take and/or store video or images of pupils. The School will provide devices to be used at school events or on school trips.

Enlisting parents' support

- Parents' attention will be drawn to the school e-Safety policy via More News, the school prospectus and school website.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden as is videoing or taking photographs of others without consent.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible

Monitoring Internet Use

The school uses a separate monitoring system (Policy Central) which staff (generally expected to be pastoral and HOD's) may use to ensure that students are complying with the Acceptable Usage Policy and are using the internet in a safe manner. Policy Central will also monitor staff usage for the same purposes but this usage will be monitored and evaluated by the Headteacher.

- All websites accessed by an individual (staff and students) will be automatically logged and this information can be provided to pastoral staff by the ICT Support Department on request.

E-mail

- Students may only use approved e-mail accounts on the school system (PMail). In the future, students may be provided with school e-mail accounts that are able to interact with external recipients. Sixth Form students may be provided with temporary access to personal web based email for the sole purpose of completing UCAS and other university/education applications.

- Students are advised to tell a teacher if they receive offensive e-mail.
- Students are advised never to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Published content and the school web site

- When a student starts at the school, parents or carers will be asked for their permission for photographs of their son/daughter to be published on the school Website and electronic signage around the school building. This permission will be recorded on file.
- A student's work can only be published with the permission of the student and parent.
- The contact details on the Web site will be limited to the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Photographs that include students will be selected carefully and students' full names will not be used anywhere on the school website particularly in association with photographs.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- YouTube access will be available for staff only. Staff will be given guidance in relation to ensuring that only suitable age related content is used.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.

The school will ensure that those individuals tasked with roles and responsibilities are effective in carrying out their duties.

Protecting personal data

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

Handling e-Safety complaints

- Student misuse of the Internet will be dealt with through the behaviour and consequence system
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

Roles and Responsibilities

Insert a table outlining the various e-safety roles and responsibilities of the individuals/groups within the school

Role	Responsibility
Governors	Approval and reviewing the effectiveness of the e-safety policy
Head Teacher	• Duty of care for ensuring the safety (E-safety) of members of the school community. • Ensuring a system is in place to allow for the monitoring and support of those in school who carry out the internal e-safety monitoring role.
SLT	Receive regular monitoring reports from the E-Safety Coordinator/Officer
Head Teacher/Nominated member of SLT	Aware of the procedures to be followed in the event of a serious allegation being made against a member of staff
E-Safety Coordinator (SLT responsibility for whole school ICT)	• Ensuring that all relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. • Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies. • Ensures all staff are aware of the procedures to be followed in the event of an e-safety incident taking place. • Liaises with the Local Authority and school technical support staff. • Receives reports of e-safety incidents and creates a log of such incidents. • Reports to SLT and Governors to discuss current issues, review incident logs and filtering/change control logs.
ICT Support Manager (and Technical Support Staff)	• Ensuring that the schools technical infrastructure is regularly updated in accordance with manufacturers guidelines to minimize potential to misuse or malicious attack • Ensure that the systems/services used to support the e-safety policy are functional and maintained.
Teaching and Support Staff	• Ensure they are up to date on e-safety matters and current school e-safety policies and practices • Ensure they have read and signed the Staff AUP • Ensure they report any suspected misuse or problem to the E-Safety Coordinator • Ensure all digital communications with students/parents/carers is carried out on a professional level • Ensure students understand and follow the e-safety policy and student AUP
Students	• Ensuring they use the schools digital technology in accordance with the student AUP
Parents/Careers	Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events • access to parents' sections of the website / VLE and on-line student / pupil records • their children's personal devices in the school / academy (where this is allowed)