E SAFETY POLICY

Mount St Joseph Document Control Table			
Document Title:	E Safety Policy	**Author name / post:**	Director of Finance & Resources
Version Number:	1.0	**Document Status:**	Approved by SLT
Date Approved:	01 Sept 2019	**Approved By:**	SLT
Effective Date:	01 Sept 2018	**Date of next review:**	September 2026
Publication method:	Website One Drive	**Date published**	Sept 2018
Superseded Version:			

Document History		
Version	**Date**	**Notes on Revisions**
1.0	Sept 2018	Revised Policy
	Sept 2019	Reviewed by HOD – CAT – for clarity – inclusion of 'proxy avoidance website' under section Policy Decisions Authorising Internet access
	Sept 2020	Reviewed by HOD – CAT – no amendments necessary
	Sept 2021	Reviewed by HOD- CAT – minor addition - Twitter
	June 2021	Reviewed by HOD- CAT – minor addition – Online Safety Guides
	June 2023	Reviewed by the HOD – CAT – Further description added to 'proxy avoidance website'.
	July 2024	Reviewed by the HOD – CAT – further description added for "Internet use will enhance and extend learning".
	July 2025	Reviewed by HOD – CAT and the CAT LM – Current updates included

Aims

We believe that every child is uniquely created and loved by God and called by Him to fulfil a special purpose. It is our privilege to help each child to identify, nurture and use his / her talents to build a better world. To this end we will work in partnership with parents, parishes, the community of schools and with the wider community.

Principles

Online Safety Overview
Our school regards online safety as a safeguarding priority, governed by Keeping Children Safe in Education (KCSIE) 2025, the Online Safety Act 2023, and relevant UK Safer Internet Centre guidelines. Digital safety is embedded across our curriculum, pastoral systems, filtering and monitoring strategies, staff training, and DSL/leadership oversight.

Mount St Joseph is committed to providing a safe and secure environment for children, staff and visitors by promoting a climate where children and adults will feel confident about sharing any concerns which they may have as a result of online safety issues.

Mount St Joseph recognises the need to be alert to the risks posed by strangers or others who may wish to harm children in school and will take reasonable steps to lessen such risks by promotion of e-safety and acceptable use guidance that is clearly understood and respected by all.

The policy is applicable to all on and off-site activities by students whilst they are the responsibility of Mount St Joseph.

Purpose

Governance, Roles & Accountability
The Designated Safeguarding Lead (DSL) holds responsibility for digital safeguarding, monitoring e-safety incidents, and coordinating with technical leads and governors.

Governors lead on oversight of online safety—reviewing incidents, evaluating filtering/monitoring effectiveness, ensuring DSL/staff training, and aligning policy updates with KCSIE and UKSIC frameworks.

- To outline the nature of e-safety and how staff and students may identify it
- To identify simple ways in which e-safety can be reported to responsible adults
- To provide a clear policy and guidelines to enable e-safety to be tackled effectively
- The e-safety lead at Mount St Joseph is James Giblin

Guidelines
Education & Training
Online safety education is integrated into the curriculum via Education for a Connected World and embedding digital literacy across year groups. Staff receive mandatory annual training and are briefed on evolving risks (e.g., AI, digital safeguarding).

Parents and pupils are engaged via Acceptable Use Agreements, newsletters, induction, and awareness events to build shared responsibility for safe online behaviour.

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

- Staff are made aware of and students are educated in the safe use of the internet
- Clear boundaries are set and discussed with staff and students, for the appropriate use of the Internet and digital communications.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students are made aware of the ever-changing landscape of AI, are taught its uses and warned against its use for plagiarism.

Students will be taught how to evaluate Internet content

- Mount St Joseph will ensure that the use of Internet derived materials by staff and by students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Managing Internet Access Information system security

- The school's ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E-mail

- Students and staff should only use approved school e-mail accounts.
- Students must be made aware of how they can report abuse and who they should report abuse to.
- Students must report any offensive or inappropriate e-mail they receive to a member of staff.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider recommending a standard mail format for all users.
- The forwarding of chain letters is not permitted.
- Staff must use the school e-mail account for communicating electronically regarding school business.
- The use of school e-mail is solely for professional use.
- Staff must follow additional steps to ensure sensitive data is secure when sending information via e-mail.

Published content and the school web site

- Staff or student personal contact information will not be published. The contact details given online are to the school office or reception.
- The Director of Finance & Resources will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images

- Photographs that include students will be selected carefully so that images of individual students cannot be misused.
- Students' full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.
- Written permission, using the approved permission form, from parents or carers will be obtained before photographs of students are published on the school website.

Social networking and personal publishing

The school will educate people in the safe use of social networking sites, and educate students in their safe use. Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- The Computing department will be responsible for frequently sharing with parents/carers online safety guides on Twitter and around school, which highlight a number of risks such as in-game purchases, inappropriate content and possible exploitation.
- Students must be made aware of how they can report abuse and who they should report abuse to.
- Students should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Students should be advised about security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- Staff are advised not to run social network spaces for student use on a personal basis.
- Staff will be advised not to include school related contacts (parents, students or ex-students) on their social network space.
- The discussion of work-related matters/information by staff, on a social network site is forbidden and would become a disciplinary matter for those who breached this principle.
- Staff may not upload school images of students onto their social network site, and would become a disciplinary matter for those who breached this principle.
- Staff must be aware that information stored, displayed or discussed on social networking sites are in the public domain.
- Staff must not upload images or full names of students, on their Departmental Twitter account that reveals the student's identity.
- Parents, students and staff should be aware that bullying can take place through social networking sites. (see section below)

Managing monitoring and filtering

Filtering, Monitoring & Emerging Technologies
We ensure robust filtering and monitoring, which now includes generative AI tools, evaluated via a "Plan Technology for Your School" approach. Systems are reviewed regularly for effectiveness, balancing the need for protective restriction with access to appropriate educational content.

Online safety practice aligns with the Online Safety Act 2023, including risk assessments and design accountability where third-party platforms are in use.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or students discover an unsuitable site, it must be reported to the E-Safety Lead or the IT Manager.
- Logs of internet breeches are kept and reviewed. Access to any illegal, suspicious websites will be reported to the appropriate agencies.

Managing videoconferencing

- Staff will establish dialogue with other conference participants to assess the risk, before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material suitable for the class.

Managing emerging technologies

Mobile Devices & Smartphone Use
We discourage non-educational smartphone use during school hours and on school trips—but recognise that outright bans may limit access to beneficial tools and digital learning. We therefore adopt context-sensitive, digitally literate strategies rather than blanket prohibition, in line with academic advice and current debate. Should legislation be enacted, we will adapt policy accordingly.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leaders are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Where contact with Students is required to facilitate their learning, staff will be issued with a school phone.
- The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- The use of mobile phones during lessons is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.
- Any personal or financial data transferred electronically should be encrypted or password protected.

Policy Decisions Authorising Internet access

- All staff and visitors must read and sign the 'Staff Acceptable Use Policy.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the school's student Acceptable Use policy.
- Students must not download unsuitable content or use proxy avoidance websites.

Assessing risks

Handling e-safety complaints

Incident Response & Review
All e-safety concerns—such as cyberbullying, harmful/challenging content, breaches of filtering, or misuse of technology—are logged and escalated via the DSL to relevant safeguarding channels. Lessons learned inform updates to the Online Safety Policy and technical measures.

We maintain a structured online safety incident log, reporting regular summaries to governors for governance and improvement.

- Complaints of Internet misuse will be reported to the e-safety Lead.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO within one working day in accordance with Bolton Safeguarding Board policies.
- Any complaint about staff misuse must be referred to the Headteacher and if the misuse is by the Headteacher it must be referred to the chair of governors in line with the school's Safeguarding and Child Protection procedures.
- Students, parents and staff will be informed of the complaint's procedure.

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective. The Trust will ensure monitoring software and appropriate procedures are in place.

Communicating E-Safety

Introducing the E-safety policy to students

- E-Safety rules will be with students all rooms where computers are used. All system users will be informed that network and Internet use will be monitored.
- A programme of E-Safety training and awareness raising will be put in place as part of the pastoral programme.

Staff and the E-Safety policy

- All staff will be given access to the school's E-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school E-safety Policy will be provided as required.

Parents' and carers' support

- Parents' and carers' attention will be drawn to the school's E-Safety Policy in newsletters and on the school's website.
- The school will maintain a list of E-safety resources for parents/carers.