MOUNT ST MARY'S CATHOLIC HIGH SCHOOL

Educating the Individual for the Benefit of All

E-SAFETY POLICY

MSM E-Safety Policy

Adopted by Mount St Marys' Governing Body on 20 September 2022

Signed  Chair of Governors

Review date: 20 September 2025

CONTENTS

Section 1

Overview

This policy should be read in conjunction with the MSM Acceptable Use Policy, MSM Bring Your Own Device Policy, MSM Data Protection Policy and the MSM Child Protection Policy.

ICT and the internet are essential tools for learning and communication that are used in Mount St Mary's Catholic High School (MSM) to deliver the curriculum, and to support and challenge the varied learning needs of its students. ICT is used to share information and ideas with all sections of the school community.

At MSM the use of the internet and ICT is seen as a responsibility and it is important that students and staff use it appropriately and practice good e-safety. It is also important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.
E-safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance applies to all staff employed either directly or indirectly by MSM as well as volunteers and staff not employed directly by the school but based at the school. All staff are expected to adhere to this code of practice to ensure the-safety of the vulnerable students, young people and adults with whom they may come into contact in their professional role. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action which could result in criminal prosecution.

Section 2

Responsibilities

MSM staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times. Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Child Protection Policy and Procedures.

Staff are solely responsible for any and all content on their own personal social media networks and electronic devices and for the security and privacy settings on social media and on all their devices, including the setting of high strength passwords which MSM recommends to be at least 6 characters and a mixture of capital and lower case letters, numbers and symbols, failure to do so may lead to disciplinary action should their actions be found to be in breach of school expectations of professional conduct by bringing the school into disrepute. Personal profiles on social networking sites and other internet posting forums should not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential, damaging to the school or undermines

public confidence in the school's reputation. All postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures which you would be happy to share with any group of friends, strangers or colleagues.

Staff must not employ any form of electronic communication to establish or seek to establish social contact with students for the purpose of securing a friendship, in response to overtures initiated by a student or to pursue or strengthen a relationship with students. Whilst the scope of this policy refers specifically to e-safety, the same practice must be strictly avoided under any circumstance or situation. If contact occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued. Staff should alert the Headteacher of any such contact immediately. All staff communication with students should always be on a professional basis, except in exceptional circumstances. When using social media of any type, staff must always remain vigilant about being certain about the identity of whom they are in communication with.

Staff should not give, nor be required to give, their personal details such as home or mobile number, social media identities or personal email addresses to students except in exceptional circumstances, as this could be construed as encouraging communication with students with unclear intentions. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent of the Headteacher may be subject to disciplinary action which could result in criminal proceedings. E-communication with students should only be done via an official school assigned staff email.

Section 5

Inappropriate Material

When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution. By avoiding the latter, the former will never be an issue.

Illegal Material

It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven could lead to consideration of the individual being barred from work with students.

Material which incites hate, harm or harassment

There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals, which includes cyberbullying by mobile phone and social networking sites

etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Professionally Inappropriate Material

A person should not use equipment belonging to their organisation to access adult pornography, as this is considered inappropriate material; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students.
Individuals need also to be mindful of actions outside the work place that could be considered so serious as to fundamentally breach the trust and confidence in the employee, which could also result in disciplinary action. Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues on social networking sites;
- Accessing adult pornography on work based computers at any time;
- Making derogatory comments about students or colleagues on social networking sites or in emails;
- Posting unprofessional comments about one's profession or workplace on social networking sites;
- Making inappropriate statements or asking inappropriate questions about students on social networking sites;
- Trading in fetish equipment or adult pornography;
- Contacting students by email or social networking without senior staff approval.

Also, always remember that if an individual finds material or behaviour offensive then effectively it is.

Section 6

Creating Images of Students through Video or Photography

Many work based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, age appropriate consent must be gained from legal guardians or students and in some instances senior management should be consulted prior to creating any images of students.

Photographic or video images must be created using MSM equipment only, except in exceptional circumstances and in such cases the images should be downloaded onto MSM equipment as soon as possible and deleted from the recording equipment immediately. In general, it should always be assumed it is not acceptable to record images of students on personal equipment such as personal cameras, mobile phones or video cameras. Images of students must not be created or stored for personal use.
Images or videos should not be displayed on websites, in publications or in a public places without such consent. The definition of a public place includes areas where visitors to the school or service provision have access.

Members of staff creating or storing images of students using personal equipment without prior consent, or being found to be recording photographic or video images for personal use, will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of students in their possession;
- ensure that students for whom permission to record photographic or video images has been withheld or withdrawn are neve in camera shot;
- avoid making images in one to one situations.

In summary
Staff are required to take steps to protect themselves and their personal information by:

- Avoiding using their personal devices for work and in work where possible
- Keeping all passwords secret and protecting access to their online accounts
- Not befriending students and young people on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and students and young people
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident including cyberbullying
- Keeping evidence of any incident including cyberbullying
- Promptly reporting any incident using existing routes for reporting concerns.

Staff in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.
Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.
For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association, from Teacher Support Network, or other organisation (move to AUP)

Further information and advice regarding cyberbullying can be found in the DfE guidance document Preventing and Tackling Bullying 2017.