MARICOURT CATHOLIC HIGH SCHOOL & SIXTH FORM CENTRE

ONLINE SAFETY AND SOCIAL MEDIA POLICY

Mission Statement

“Our Maricourt family, with Christ at the centre, is a community of welcome, compassion and respect in which we are encouraged to discover our true purpose and empowered to achieve the extraordinary so as to be the change we want to see in our world.”

INSPIRE WITH MARICOURT

POLICY REVIEWED: September 2022
SCHEDULED REVIEW: September 2023

Contents

Creating an Online Safety Ethos

Aims and policy scope

Maricourt Catholic High School believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Maricourt Catholic High School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Maricourt Catholic High School has a duty to provide the school community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Maricourt Catholic High School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of this online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Maricourt Catholic High School is a safe and secure environment.
- Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (RSE). Also the staff code of conduct.

Writing and reviewing the online safety policy

The Designated Safeguarding Leads (DSLs) are Mr D Friend, Mr I Daly, Mrs D Lawler Mr S Naughton.

The school Online safety lead is Mr C Marsh.

Key responsibilities for the school

The key responsibilities of the school Governors and senior leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy and staff Code of Conduct which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To ensure resources are in place to enable technical staff in monitoring the safety and security of school/ systems and networks.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead.

The key responsibilities of the Designated Online Safety Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- To report to the designated safeguarding lead and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.

- Working with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Work with DSL to ensure that online safety is integrated with other appropriate school policies and procedures i.e. anti-bullying policy and behaviour.
- Leading an online safety team/group with input from stakeholder groups.

The key responsibilities for all members of staff are:

- Contributing to the implementation of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

The key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

The key responsibilities of children and young people are:

- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- At a level that is appropriate to their individual age, ability and vulnerabilities:
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Online Communication and Safer Use of Technology

Managing the school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The head teacher/manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

Publishing images and videos online

The school will ensure that all images and videos shared online are used in accordance with the school image use policy.

The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.

The school has an active social media presence. All members of the school community can contribute to the feed and may request for posts to be removed.

Managing email

- Pupils may only use school provided email accounts for educational purposes**.**
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail is blocked through the school filter.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts is blocked for pupils.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Official videoconferencing use for educational purposes

- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publicly.

- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels for example Zoom, Teams, Google Meet, Skype.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools. The Smoothwall will *always* turn on the safe search function.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Management of school learning platforms/portals/gateways

- The VLE is regularly monitored by the network manager.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content on the VLE will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the VLE for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the VLE by a member of the leadership. In this instance there may be an agreed focus or a limited time slot. The visitor will be supplied with a guest account and monitored password.

Social Media Policy

General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- The school will not tolerate any form of abuse, threats or violence online. Appropriate action will be taken towards any stakeholder who causes defamation of character, causes distress or anxiety. The school will take reasonable action towards any harassment, (repeated attempts to impose unwanted communications), bullying or jeopardises the safety, mental health or reputation of any member of the Maricourt Community. The school will liaise with the Police if the law has been broken and will work in line with the Behaviour and Anti-bullying policy.

- All members of the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.

- All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.

The use of social networking applications during school hours for personal use is not permitted, Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.

Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as the staff code of conduct, anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Official use of social media

- School's current official social media channels are Instagram, Facebook and Twitter

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

- Any online publication on official social media sites will comply with legal requirements including the General Data Protection Regulation 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

- Official social media use will be in line with existing policies including anti-bullying and child protection.

- Images or videos of children will only be shared on official social media sites/channels in accordance with parental permission.

- Students, staff and parents can request for posts to be removed.

- Social Media should not be used to complain or air negative opinions or thoughts about the school. Complaints should be made via the official school channels. (See complaints policy)

Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed as part of the staff Code of Conduct with all members of staff, as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- All members of staff are *advised* not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.

- All communication between staff and members of the school community on school business will take place via official approved communication channels.

- Staff are *advised* not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.

- Members of staff will be encouraged to manage and control the content they share and post online.

- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

- Members of staff are *advised* not to identify themselves as employees of Maricourt Catholic High School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and also to safeguard the privacy of staff members and the wider community.

Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school/setting (see Staff Code of Conduct).

- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.

- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

- Staff must ensure that any image posted on any official social media channel have appropriate parental consent.

- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online. Staff should not personally retaliate.

- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

Pupils use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.

- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

- Any official social media activity involving pupils will be moderated by the school where possible.

- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.

- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Personal Devices and Mobile phones

Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use or Mobile Phone Policy. School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.

- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school/ accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.

- Members of staff will be issued with a work phone number and email address where contact with pupil or parent/carer is required.

- All members of the school community will be *advised* to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.

Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.

- Pupil's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons.

- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

- Pupils are not allowed to contact their parents via their mobile phone during the school day, but to contact the school office.

- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy. Students will receive negative behaviour points for using mobile phones on school site.

- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be

deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy.

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

Staff use of personal devices and mobile phones

- Members of staff are *not advised* to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

- Staff are *advised* not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

- Staff who use a personal mobile phone devices to contact home should always call with a private caller ID.

Policy decisions

Reducing online risks

- Maricourt Catholic High School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

- Emerging technologies will be examined for educational benefit and the network manager will ensure that appropriate risk assessments are carried out before use in school is allowed.

- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

- The school will audit technology use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's network manager.

Internet use throughout the wider school/setting community

- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

Engagement approaches

Engagement and education of children and young people

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.

- Assemblies will also be delivered to pupils to create a culture of keeping safe on-line and also educate students on how to reduce risks.
- The school website will be updated with advice and information on how to keep safe on line for both pupils and parents.
- Online safety education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations are displayed on computer screens.
- External support will be used to complement and support the school's internal online safety education approaches.

Engagement and education of staff

- The Online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.

Engagement and education of parents and carers

- Maricourt High School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This will include offering a parent information with demonstrations and suggestions for safe home Internet use or highlighting online safety.
- Parents will be requested to read online safety information as part of the Home School Agreement.

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

Managing information systems

Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices.

Filtering and Monitoring

- The network manager will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of the community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity.
- The school uses a Smoothwall firewall which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Network Manager and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies.

Management of applications (apps) used to record children's progress

- Apps/systems which store personal data will be risk assessed prior to use.
- Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Personal staff mobile phones or devices are not advised to be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

Responding to Online incidents and Safeguarding concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Online Safety Lead will be informed of any online safety incidents, which will then be recorded.
- The DSL will ensure that online safety concerns involving child protection are escalated and reported to relevant agencies in line with the Sefton Safeguarding Children Board thresholds and procedures.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Headteacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- Parents and children will need to work in partnership with the school to resolve issues.

Procedures for responding to Specific Online incidents or concern

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Maricourt High School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").

- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils (within the curriculum), staff (via INSET) and parents/carers (via the information evening).

- Maricourt High School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads.

- The school will follow the guidance as set out in the non-statutory UK Council for Child Internet Safety (UKCCIS) advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and "Responding to youth produced sexual imagery" guidance which compliments the statutory Keeping Children Safe in Education (KCSIE) guidance.

- If the school are made aware of incident involving creating youth produced sexual imagery the school will:

    - Act in accordance with the school's child protection and safeguarding policy Sefton's Safeguarding Child Boards procedures.

    - Immediately notify the DSL.

    - Store the device securely.

    - Carry out a risk assessment in relation to the children(s) involved.

    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies).

    - Make a referral to children's social care and/or the police as needed when appropriate.

    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.

    - Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.

- Review the handling of any incidents to ensure that the school is implementing best practice and the DSL will review and update any management procedures where necessary.

- Inform parents/carers about the incident and how it is being managed.

- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).

- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.

- If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.

- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Maricourt High School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils (within the curriculum), staff (via INSET) and parents/carers (via the information evening).

- Maricourt High School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the LADO and/or Police.

- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the Police by the DSL.

- If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the school's child protection and safeguarding policy and Sefton's Safeguarding Children Boards procedures.
- Immediately notify the DSL
- Store any devices involved securely.
- Immediately inform the Police (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the DSL will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the LSCD/LADO to enable other schools to take appropriate action to safeguarding their community.

Responding to concerns regarding Indecent Images of Children (IIOC)

- Maricourt High School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the LADO and/or Police.

- If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:

    - Act in accordance with the school's child protection and safeguarding policy and the Local Safeguarding Children's Boards procedures.

    - Immediately notify the school DSL.

    - Store any devices involved securely.

    - Immediately inform appropriate organisations and/or the Police (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:

    - Ensure that the DSL is informed.

    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

    - Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:

    - Ensure that the DSL is informed.

    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

    - Ensure that any copies that exist of the image, for example in emails, are deleted.

    - Inform the Police (999 if there is an immediate risk of harm) and Children's Social Care (as appropriate).

- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

  - Ensure that the DSL is informed or another member of staff in accordance with the school whistleblowing procedure.

  - Contact the Police regarding the images and quarantine any devices involved until Police advice has been sought.

  - Inform the (LADO) and other relevant organisations in accordance with the schools managing allegations policy.

  - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding Radicalisation and Extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which considers the needs of pupils.

- When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the safeguarding policy.

- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the LSCB or Police.

Responding to concerns regarding Cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

- All incidents of online bullying reported will be recorded.

- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the LCSB and/or Police.

- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding online hate

- The act of online hate will not be tolerated at Maricourt High School. Further details are set out in the school policies regarding anti bullying and behaviour.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the LCSB and/or Police.

Online Safety contacts and references

Support and Guidance

Sefton Local Safeguarding Children Partnership: Sefton Local Safeguarding Children Partnership - scp (seftonscp.org.uk)

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

National Online Safety: https://nationalonlinesafety.com/