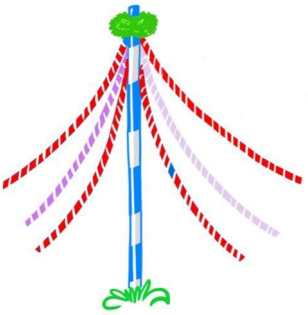
Maypole School



E-SAFETY POLICY

September 2023

Drafted by:	John Herring	
Authorised by:	Adrienne Cherrywood	04 Sep 2022
Publication Date:		05 Sep 2022
Reviewed:	Adrienne Cherrywood	29 June 2023
Next Review due:		01 Aug 2024

CONTENTS

1. INTRODUCTION

Paramount importance of safety

Maypole School is committed to providing outstanding educational opportunities for all our pupils. The safety and welfare of our pupils is of the utmost importance. Ensuring that pupils can safely access new technology, and learn how to participate in the digital world without compromising their safety and security, is a key part of delivering a well-rounded programme of education.

This policy sets out how we will keep pupils at Maypole School safe, whether using new technology in the school, when offsite or at home, including accessing remote learning.

Legislation and guidance

This policy has been written with reference to a range of guidance including Keeping Children Safe in Education (DfE, 2023), 'Teaching online safety in schools' (DfE, 2023), the 'Education for a Connected World' framework (UKCIS, 2020), 'Relationships and sex education (RSE) and health education (DfE, 2021), the London Grid for Learning (LGfL) E-Safety Policy and the South West Grid for Learning (SWGFL) E-Safety Policy. The policy is also informed by government guidance on the Prevent duty and Channel.

E-safety represents a crucial strand of safeguarding children and vulnerable adults, and as such this policy should be read in conjunction with Maypole School's Child Protection and Safeguarding Policy and Procedures, as well as the related policies and procedures listed at the end of this policy.

Who this Policy applies to

This policy applies to all members of the Maypole School community including staff, pupils, volunteers, families, visitors and external professionals.

2. THE RISKS & DANGERS OF DEVELOPING TECHNOLOGY

The impact of technology on the lives of all citizens increases yearly, particularly for children and young people who are keen to explore new and developing technologies.

Categories of risk and danger

Technology is transforming the way that schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. Developing technology brings opportunities; it also brings risks and dangers. Keeping Children Safe in Education (2023) categorises these as:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

The risks to pupils using new technologies

Within these categories, risks to pupils using new technologies may include, but are not limited to:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Internet grooming
- Extremism and radicalisation
- Child criminal exploitation (CCE) and/or child sexual exploitation (CSE)
- The sharing and distribution of personal images without consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Sexting
- Access to unsuitable video and internet games
- Misinformation and disinformation
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use which may impact on social and emotional development and learning

3. ROLES AND RESPONSIBILITIES

E-Safety Lead, and Designated Safeguarding Lead (DSL)

Maypole School's named E-Safety Lead is Kitty Clark, Executive Headteacherl and Designated Safeguarding Lead (DSL) who will work with the Deputy DSL to oversee and manage the recording, investigation and resolution of cyberbullying and any other incidents which fall within the remit of this policy.

The Executive Headteacher

The Executive Headteacher will monitor the impact of this policy using:

- Logs of reported incidents (maintained by the E-Safety Lead).
- Monitoring of the school's network where necessary.
- Regular monitoring of the school's social media presence.
- Monitoring of all remote learning platforms where necessary, including Google Meet; Zoom; Microsoft Teams.
- Monitoring of the school's internet access where necessary, and regular reviews of the school's website filtering.
- Have responsibility for ensuring all staff undergo training in and understanding roles and responsibilities in relation to filtering and monitoring, both at induction and annually.
- Parent/carer questionnaires.

Safe delivery of ICT

The school supports the development and delivery of ICT through Computing lessons, digital workshops and initiatives. Pupils are supported to use games appropriately and only in designated time slots. The school also works with pupils around the dangers of online gaming and meeting people online, as well as risks relating to 'fake news' and other misinformation/disinformation including conspiracy theories and uses resources to support pupils with SEND to understand these topics.

All staff

All Maypole School staff will familiarise themselves with this policy. E-safety is included in discrete lessons and throughout the year through other vehicles, such as assemblies and themed activities e.g. Anti-Bullying Week. Staff are reminded of their e-safety obligations via regular updates, training and discussion throughout the year.

Pupils at the school are not allowed to use their own mobile phones or tablet/laptop devices to use in school, and all staff are to enforce this. Each pupil has access to a tablet or Chromebook provided by the school for use during the school day.

Governing Body

Maypole School's Governing Body will monitor adherence to the policy, together with the E-Safety Lead, and will be an agenda item at governing body meetings.

4. CREATING A SAFE ICT INFRASTRUCTURE

Access rights

All users of Maypole School computer networks have clearly defined access rights, managed via a username and password login system. Account privileges are based upon each user's agreed requirements. Pupil accounts are restricted, and do not allow access to all network drives. Guests are required to log in using a visitor login, that has limited network access.

Internet filtering and security software

A permanently-enabled filtering system is used to filter inappropriate material. Additionally web pages are scanned for content as requested. Any changes to settings have to be requested through the school's IT Helpdesk. All changes made to Internet filtering are logged. Security software is installed on all computers.

Internet monitoring

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential.

Please refer to the Maypole School IT Acceptable Use Policy for further details.

5. E-SAFETY RULES

Rules for publishing material online (including images of pupils)

Maypole School's website is a valuable tool for sharing information and promoting pupils' achievements. But we recognise the potential for abuse. Therefore the following principles will always be considered:

- **No use of pupil surnames**. If an image, video or audio recording of a pupil is used, their surname must not be used (including in credits).
- **Pupils use of their own surnames online**. Children and young people use a variety of online tools for educational purposes. They will be asked to only use their first name for any work that will be publicly accessible and will be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.
- **No photos of pupils on personal devices**. Staff **must not** take photographs of any pupils using their personal devices – all pupil photographs must be taken using Maypole School's equipment and transmitted through the school's systems.
- **No surnames in File names**. Files should be appropriately named in accordance with these principles.
- **Suitable clothing**. Only images of pupils in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- **Parental permission**. Parents/carers are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school's website or any publicity material.
- **Intellectual property**. Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- **Content**. Content should be polite and respectful.
- **Leadership Team check before any publication**. Material should be checked by a member of the school's Leadership Team before being published.
- **Personal social media accounts**. Staff must not post or transmit images of pupils or families via their personal social media accounts. Maypole School considers social media to be any technology-based platform used for interacting or discussion via voice, text, video or pictures. Please refer to the Social Media Policy for further information.
- **Employees permission**. Employees should not post any images of other Maypole School staff on any social media without first obtaining permission from those person(s) in the image.
- **Photos and videos taken by parents / carers**. When photos and videos of Maypole School events are permitted to be taken by parents and carers, they will be asked not to publish them on any public area of the Internet, including social networking sites. There will be events when the taking of photos or videos will not be permitted.

Pupil rules for acceptable internet use

We will adopt the rules as laid out below in an age-appropriate way for the pupils at Maypole School.

- *I will ask permission from an adult before using the Internet.*
- *I will use computers and tablets safely.*
- *I will not look for websites that I know I'm not allowed to see.*
- *If I see anything that I know is wrong I will tell an adult straight away.*

- *I know that I can talk to an adult if I see or experience anything on the Internet that makes me feel scared or unhappy.*
- *I will not download anything without permission from an adult.*
- *I will not use memory sticks on school computers without permission from an adult.*
- *I will ask an adult before sending emails.*
- *I will be polite and respect others when using the Internet.*
- *I will not give out any personal information over the Internet.*
- *I will not share my login details with others.*
- *I understand that the school may check my computer files and check what I am doing.*
- *I will not upload to social media any photos, videos or sound recordings that contain other pupils or staff within the school.*

Visitor rules for acceptable internet use

Visitors' Internet use will vary depending upon the purpose of their visit. Generally we expect all visitors to abide by the following rules:

- *I will respect the facilities by using them safely and appropriately.*
- *I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.*
- *I will not deliberately seek out inappropriate websites.*
- *I will report any unpleasant or upsetting material to a member of staff immediately.*
- *I will not download or install programme files.*
- *I will not use USB memory devices on school computers.*
- *I will be polite and respect others when communicating over the Internet.*
- *I will not share my login details.*
- *I will not carry out personal or unnecessary printing.*
- *I understand that the school may check my computer files and monitor my Internet use.*
- *I will not make or share defamatory posts relating to the school on any social media.*

Staff/Governing Body Member rules for acceptable Internet use

Staff and governing body members must use the Internet safely, appropriately and professionally within the school and when conducting any school business or representing the school outside of the school environment. They must be aware that they are role models for others and are expected to promote and model high standards of behaviour at all times. For further details please refer to the school's IT Acceptable Use Policy.

6. E-SAFETY EDUCATION AND TRAINING

E-Safety education

The aim of e-safety education within Maypole School is to teach pupils how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Pupils will be taught about safe and appropriate electronic communication, including the indelible nature of emails, social media presence, images and other e- communications. Aspects of e-safety such as cyberbullying, revenge porn, trolling and other harassment will be covered in an age-appropriate way, with emphasis placed on respecting oneself and one's peers, in order to build confidence and understanding among pupils as they interact with technology.

Younger pupils

For younger pupils Internet use will be closely supervised and based around pre-selected, safe websites. Pupils will be regularly reminded about how to always take care when clicking and to seek help from an adult if they see anything that makes them unhappy or that they are unsure about. These digital literacy skills will be developed in keeping with pupils' age and ability, with lessons promoting a responsible attitude towards searching the Internet and the importance of personal security measures such as strong passwords and processes for reporting any concerns.

Independence skills

As they progress through the school, pupils will be encouraged to become more independent at researching information on the Internet, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported to use online collaboration tools for communicating and sharing ideas.

E-Safety Updates for Parents/Carers

Maypole School provides opportunities for parents and carers to receive e-safety education and information (e.g. via the website and/or newsletters) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety.

Do's and Don'ts for Staff - How to stay 'Cybersafe'

There is a comprehensive list of Do's and Don'ts for Staff, at Appendix 1.

E-Safety Updates for Staff

Staff receive regular updates about how to protect and conduct themselves professionally online and to ensure that they have an awareness of issues surrounding modern technologies, including safeguarding. Updates are delivered through CPD, staff meetings, email updates and via the staff Sharepoint, which also signposts to relevant external resources and sources of support.

7. USE OF SOCIAL NETWORKING & MESSAGING SYSTEMS

Maypole School recognises that many staff will actively use Facebook, Twitter and other social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Confidentiality and professionalism

Staff must recognise that it is not appropriate to discuss issues relating to pupils or colleagues via social media networks; discretion and professional conduct is essential. Posts that bring Maypole School into disrepute and/or breach confidentiality are likely to result in disciplinary action. Staff must review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

Engagement with current and ex-pupils

It is never acceptable to accept a friendship request from a child or young person at Maypole School or from ex-pupils who are still minors or have left the school within the last five years. This is to avoid any possible misinterpretation of motive or behaviour which could be construed as grooming. In the event that a pupil or ex pupil makes, or tries to make, contact with you it is essential that you report this to the Head Teacher or Principal.

Personal contact details

Staff must not give their personal contact details to pupils or parents/carers, including e-mail, home or mobile telephone numbers. All correspondence should be via Maypole School systems.

Please refer to the Social Media Policy, the Staff Code of Conduct and the IT Acceptable Use Policy for further details.

8. DATA PROTECTION

Personal data and GDPR

Personal data will be recorded, processed, transferred and made available according to the principles of the General Data Protection Regulation (GDPR), which state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Actions required by Staff

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly ‘logged-off’ or ‘locked’ at the end of any session in which they are using personal data;
- Be fully aware of the risks of transferring data using removable media. When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete.

Sending confidential information safely

It may sometimes be necessary to send confidential information outside the organisation, for example as part of a safeguarding investigation, or when sending documents to an SEN team in a Local Authority.

Maypole School staff must at all times consider the security of such information. Any confidential or sensitive information conveyed via email outside of the school systems must be encrypted. Where encryption is not available, information must be password protected and the password conveyed separately to the recipient, preferably by means other than email.

9. E-SAFETY FOR PUPILS AND STUDENTS ACCESSING REMOTE OR BLENDED LEARNING

Maypole School recognises that pupils and students may experience periods where they are unable to attend school, whether due to external factors such as the ongoing coronavirus outbreak or as a result of their additional needs / complex health issues. These pupils will be supported to access remote or blended learning as necessary, with appropriate safeguards in place.

Providing information about staying safe online

When pupils are not able to attend school for a period of time, the risks associated with online activity including remote learning are potentially heightened. When sending work home to pupils currently unable to attend, school staff include information on staying safe online and sources of support, including reporting pathways, where pupils have concerns about online activity. This includes details of Safeguarding teams, as well external agencies including:

- **Childline** – for support
- **UK Safer Internet Centre** – to report and remove harmful online content
- **CEOP** – for advice on making a report about online abuse

School websites are also kept updated with relevant links and other e-safety information for both pupils and families.

When setting home learning, Maypole School ensures any use of online learning tools and systems is in line with privacy and data protection / GDPR requirements.

Procedures for delivering remote learning

Maypole School operates clear procedures around delivering remote learning, including the following key points:

- **Staff Code of Conduct.** Staff must adhere to the Maypole School Staff Code of Conduct **at all times**, including when delivering remote learning.
- **Risk assessment**. When planning delivery of live sessions, staff should consider the needs and profiles of each pupil intended to receive the session, and risk assess accordingly.
- **Standards of dress**. Staff and children/young people must wear suitable clothing, as should anyone else in the household.
- **Blurred backgrounds**. Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- **Length of live classes**. Live classes should be kept to a reasonable length of time, or the streaming may prevent the family ‘getting on’ with their day.
- **Appropriate language**. Language must be professional and appropriate, including any family members in the background.

- **Approved platforms only**. To communicate with pupils, Staff must only use platforms specified by senior managers and approved by the IT network manager/provider
- **Record of attendance**. Staff should record the length, time, date and attendance of any sessions held.
- **Ongoing discussion of online safety**. Staff maintain regular contact with all pupils not currently attending, and this provides a further opportunity to discuss online safety with them, their parents and carers. We are aware that when a pupil is unable to attend school for any length of time, families may wish to access additional home learning support, for example tutors or other specialists, and staff emphasise the importance of securing online support from reputable organisations/individuals who can provide evidence that they are safe and can be trusted to have access to children or vulnerable adults.

10. RELATED POLICIES AND DOCUMENTATION

The following Policies are relevant to this policy, and may need to be referred to.

- Anti-Bullying Policy
- Prevent Policy
- Child Protection and Safeguarding Policy and Procedures
- Data Protection Policy and related documentation
- IT Acceptable Use Policy
- Positive Behaviour Policy
- Online & Blended Learning Policy
- Social Media Policy
- Staff Code of Conduct

APPENDIX 1: HOW TO STAY 'CYBERSAFE' – STAFF DO'S AND DON'TS

DOs

- **Be careful about your online reputation**. Be aware of your online reputation, which consists of information you post about yourself and information posted by others. Remember that when seeking future employment, many prospective employers will use publicly available online information. Remember, the internet never forgets.
- **Passwords**. Keep your passwords confidential and protect access to accounts.
- **Privacy settings**. Regularly review your privacy settings.
- **Avoid misunderstandings**. Discuss expectations with friends – are you happy to be tagged in photos, for example?
- **Legal evidence**. Be aware that, increasingly, individuals are being held to account in the Courts for the things they say on social networking sites.
- **Keep personal phone numbers private**. Keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents/carers.
- **Use school mobiles**. Use a school mobile phone for all school business.
- **Your IMEI number**. Keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible.
- **Enforce school rules**. Ensure that school rules regarding the use of technologies are consistently enforced.
- **Report any incident**. Report any incident to the appropriate member of staff in a timely manner.
- **Preserve all evidence**. Keep any evidence of an incident, for example by not deleting text messages or emails, and by taking a screen capture of material, including the URL or web address.
- **School email address**. Use your school email address only for work purposes.
- **Personal email accounts**. Be aware that if you access any personal web-based email accounts via the Maypole school network, these may be subject to the school's internet protocol which could include monitoring and surveillance.
- **Act on any concerns you may have**. Do raise any genuine concerns about the school, or about specific members of staff, using the Whistleblowing or Grievance procedures.

DON'Ts

- **Post private or sensitive information**. Don't publicly post information and photos about yourself, or Maypole school related matters, that you wouldn't want employers, colleagues, pupils or parents/carers to see.
- **Befriend or interact with pupils on social media**. Don't befriend pupils or other members of the school community on social networking sites.
- **Befriend or interact with ex-pupils**. Don't befriend parents/carers or ex-pupils
- **Retaliation**. Don't personally retaliate to any incident or bullying messages.
- **Don't criticise others online**. Don't criticise Maypole School, or pupils or their parents/carers online.