DO IT WITH THY MIGHT

MALDON COURT

PREPARATORY SCHOOL

7h

E-Safety Policy

This Policy applies to all children at Maldon Court Preparatory School including those in the EYFS

Reviewed and Updated September 2023 Mrs K Abrehart

To be reviewed – September 2024

School Aims

- Children develop a love of learning and come to appreciate the value of their talents and life experiences.
- Children flourish and become enthusiastic and independent learners reaching their full potential through a stimulating, broad curriculum and rich variety of experiences beyond the curriculum.
- Children embrace the traditional values of Kindness, Respect and Courtesy, becoming responsible, independent caring individuals.
- Children are confident happy individuals who are well prepared for their next step in education. This includes 11+, scholarships and entrance to schools with Specialist Status.
- Children develop the fundamental British Values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs: both in the local and wider community.

Introduction

Maldon Court recognises that the internet and other digital technologies provide a vast opportunity for children to learn. It allows for those involved in the education of the children to promote creativity, stimulate awareness and enhance learning. As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable children to gain access to a wide span of knowledge in a way that ensures their safety and security.

It is the duty of Maldon Court School to ensure that every child in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our children are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, peer on peer abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs - Including live streaming
- Social networking sites
- Chat rooms
- Music/video downloads
- Gaming sites
- Text messaging and picture messaging

- Podcasting
- Video calls
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Agreement (for all staff, board of visitors, volunteers, children, parents and visitors), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding
- Behaviour
- Anti-Bullying
- Data Protection - Staff
- PSHE scheme of work
- RSE policy
- Taking, Storing and Using of Images
- Privacy Notice

Roles and responsibilities

The Board of Visitors

The Board of Visitors of the School are responsible for the approval of this policy and for reviewing its effectiveness. To be signed of in accordance with the Safeguarding Policy each Autumn term.

Headteacher and the Senior Management Team

The Headteacher is responsible for the safety of the members of the School community and this includes responsibility for E-Safety. The Headteacher has delegated day-to-day responsibility to the E-Safety Coordinator - Mrs Katharine Abrehart.

In particular, the role of the Headteacher and the Senior Management Team is to ensure that:

- Staff are adequately trained about E-Safety
- Staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of E-Safety in connection to the School.

E-Safety Coordinator/ICT Teacher

The School's E-Safety Coordinator is responsible to the DSL for the day to day issues relating to E-Safety. The E-Safety Coordinator has responsibility for ensuring this policy is upheld by all members of the school staff and works with the ICT subject leader to achieve this. They will keep up to date on current E-Safety issues and guidance issued by relevant organisations, including ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Essex Safeguarding Children Board. The Senior Management Team are updated by the E-Safety Coordinator at termly meetings and all Board of Visitors understand the procedures and strategies at our School in relation to E-Safety and local and national guidelines and advice. ICT and any E-Safety issues are also discussed at the Senior Management Team meetings.

Pegasus IT Ltd - 3G, 4G and 5G - Filtering/monitoring

Filtering and monitoring systems are used to keep pupils safe when using Maldon Court's IT system. Our **filtering systems** block access to harmful sites and content. Our **Monitoring systems** identify when a user accesses or searches for certain types of harmful content on school devices. We are then alerted to any concerning content.

All staff are clear on the expectations and responsibilities in relation to filtering and monitoring as part of their annual safeguarding training. For example, part of their role will be to monitor what's on pupils' screens. Staff are aware of how to report safeguarding and technical concerns, such as if:

- They witness or suspect unsuitable material has been accessed
- They are able to access unsuitable material
- They are teaching topics that could create unusual activity on the filtering logs
- There is failure in the software or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- They notice abbreviations or misspellings that allow access to restricted material

- All staff are trained in filtering and monitoring. They are aware of their role and how they can safeguard children with regards to harmful content. They are also aware of how they can protect their 365 accounts and who to raise a concern with should they identify an issue.

Senior leaders are aware of and understand:

- What provisions Maldon Court has in place and how to manage these
- How to escalate concerns
- That staff are trained appropriately and understand their role

The DSL and DDSL have lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place, this includes overseeing and acting on:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

- The school has a contract with Pegasus IT Ltd. The role of the external company is to maintain a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for advising all staff regarding the use of ICT. They monitor the use of the internet and emails including the management of 3G/4G/5G mobile networks and maintain content filters.
- The school has With-Secure Protection in place. This is centrally monitored and would send a report to the office@maldoncourtschool.org email address when an alert is triggered. This has been updated to the newest version as of September 2023.

- Additionally, all DNS requests made on the school network, are filtered through OpenDNS' Umbrella detection system, this prevents access to web pages that are harmful or inappropriate before the content is downloaded to the computer/ laptops/ personal devices or tablets. As the requests are centrally made from the server to OpenDNS' system, they cannot be traced to specific users/computers on the network for monitoring purposes.
- Any safeguarding concerns, alerted through filtering and monitoring, are communicated to the DSL. Updates from Pegasus IT Ltd regarding filtering and monitoring are relayed through both the DSL and ICT subject leader.
- All filtering and monitoring will be reviewed annually or as required.

All staff

All staff are required to sign the Acceptable Use Agreement; new staff do so as part of their induction. As with all issues of safety at this School, staff are encouraged to create a talking and listening culture in order to address any E-Safety issues which may arise in classrooms on a daily basis.

Children

Children are responsible for using the School ICT systems in accordance with the Acceptable Use Agreement and for letting staff know if they see the ICT system being misused.

Parents and carers

Maldon Court believes that it is essential for parents to be fully involved with promoting E-Safety both in and outside of School. We regularly consult and discuss E-Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about children's behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. Parents and carers are responsible for endorsing the School's Acceptable Use Agreement for Children.

Visitors including Visiting Speakers

Visitors including visiting speakers will be accompanied by the staff organiser at all times. All visitors are signed in at the school office and advised of our school safeguarding policy, they are required to turn off their mobile phones.

Education and Training

Staff - Awareness and training

New staff receive information on Maldon Court's ICT/ E-Safety Policy and Acceptable Use Agreement as part of their induction. All staff receive regular information and training on E-Safety issues in the form of INSET training and internal meeting time. They are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School E-Safety procedures. These behaviours are summarised in the Acceptable Use Agreement. When children use School computers, staff should ensure children are fully aware of and understand the agreement they have made by following the School's ICT guidelines.

Teaching staff are encouraged to incorporate E-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community. A record of concern must be completed by staff as soon as possible if any incident relating to E-Safety occurs and be provided directly to the School's Designated Safeguarding Lead Mrs E Mason or DDSL Mrs K Abrehart.

Children

E-Safety in the curriculum

ICT and online resources are used increasingly across the curriculum in line with DfE Teaching online Safety in Schools June 2019 and Education for a Connected Framework. Please see the schools PSHE and RSE policies. The School believes it is essential for E-Safety guidance to be given to children on a regular and meaningful basis. We continually look for new opportunities to promote E-Safety and regularly monitor and assess our children's understanding of it. The School provides opportunities to teach about E-Safety within a range of curriculum areas, Computer Science and age-appropriate PSHE lessons.

These include:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

Children are taught about their E-Safety responsibilities and to look after their own online safety. They are taught about recognising online sexual exploitation, stalking and grooming, the risks and of their duty to report any such instances they or their peers come across.

Children are aware of the impact of Cyberbullying and understand it will not be tolerated. Children know how to seek help if they are affected by any form of online bullying. They are also aware of where to seek advice or help if they experience problems when using the internet and related technologies. They are advised to seek help from a parent, teacher, trusted staff member, or an organisation such as Childline, NSPCC or CEOP report abuse button.

Parents

The School seeks to work closely with parents and carers in promoting a culture of E-Safety. The School will always contact parents if it has any concerns about children's behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. The School recognises that not all parents and carers may feel equipped to protect their child when they use electronic equipment at home. The School can access weekly online updates from the NOS and these are sent to parents to offer advice about E-Safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Use of personal devices (BYOD)

The School allows staff to bring in personal mobile phones and devices for their own use. Under normal circumstances, the School does not allow a member of staff to contact a pupil or parent/carer using their personal email or mobile phone number unless it is approved first by the Headteacher. Children are not permitted to bring personal mobile devices/phones to School. Children may bring into school a laptop; they may only be used for educational purposes, as agreed with the teacher. The school is not responsible for the loss, damage or theft of any personal laptops.

- The sending of inappropriate messages between any members of the School community is not allowed.
- No images, sound or videos are to be used outside of the school environment.
- No images, sound or videos are to be uploaded to any social media sites.
- Staff and children bringing personal devices or laptops into school must ensure there is no inappropriate or illegal content on the device.
- Privately owned ICT equipment can be linked to the wireless network but must not be connected to the main school network.
- In the Early Years Foundation Stage (EYFS), staff must not in any circumstances use their mobile phones to take photographs of the children. School hand-held devices must be used at all times and not be taken off site.

Use of School devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the School device which is allocated to them for School work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Staff are responsible for any activity undertaken on the School's ICT equipment provided to them.

Social Media

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with schoolwork or business from school devices or whilst in front of children. Occasional access may only be made whilst in staff-only areas of school. Staff must immediately report to the Senior Management Team the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the E-Safety Co-ordinator. Any online communications must not either knowingly or recklessly:

- Place a child or young person at risk of harm, or cause actual harm
- Bring the School into disrepute
- Breach confidentiality
- Breach copyright
- Breach data protection legislation

Do anything that could be considered discriminatory against, bullying or harassment of, any individual, for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race including nationality, disability, sexual orientation, religion or belief or age.
- Using social media to bully another individual; or
- Posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should staff add children as social network 'friends' or contact them through social media.

Staff should:

- Not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data.
- Save their data on a frequent basis to the School's network drive. They are responsible for the backup and restoration of any of their data that is not held on the School's network drive.
- Ensure portable and mobile ICT equipment is made available as necessary for antivirus updates and software installations, patches or upgrades
- Not attempt to install any applications or software packages.

Children

The School expects children to think carefully before they post any information online, repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Children must report any accidental access to materials of a violent or sexual nature directly to the class teacher who will complete the E-Safety Incident Report Form and pass it to the Designated Safeguarding Lead. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded and will be dealt with under the School's Safeguarding Policy. Children should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored.

E-mail

The use of e-mail within School is an essential means of communication for staff. In the context of School, e-mail should not be considered private.

Educationally, email can offer significant benefits including direct written contact between Schools on different projects, be that either staff based, or pupil based, within School or international. We recognise that they need to understand how to style an e-mail in relation to their age and good network etiquette. The School has taken all reasonable steps to ensure that the School network is safe and secure. The whole School community should be aware that email communications through the School network are monitored.

Managing e-mail: Staff

- The School gives all staff their own e-mail account to use for all School business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary,

e-mail histories can be traced. The School email account should be the account that is used for all School business.

- Staff must avoid contact with children, parents or conduct any School business using personal home e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on School headed paper.
- All e-mails between staff and children or parents / carers must be professional in tone and content.
- Staff sending e-mails to external organisations and parents are advised to cc. the Headteacher or class teacher.

E-mails created or received as part of staff School activities could be subject to disclosure in response to a Subject Access Request under Data Protection Law. Staff must therefore actively manage their e-mail account as follows:

- Delete all e-mails of short-term value.
- Organise e-mail into folders and carry out frequent housekeeping on all folders and archives.
- Staff must inform the Senior Management Team if they receive an offensive e-mail.
- Staff access to their School e-mail (whether directly through webmail when away from the School or on non-School hardware) will be subject to this policy.
- Use 2FA for their email accounts.

Managing e-mails: Children

Children may only use School approved accounts on the School system for educational purposes.

Sending e-mails: Staff

- Staff must use their own School e-mail account so that they are clearly identified as the author.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Not send or forward attachments unnecessarily. Whenever possible, save the attachment to the shared drive rather than sending

Receiving e-mails: Staff

Staff should:

- Check their e-mail regularly.
- Activate their ‘out-of-office’ notification when away for extended periods.
- Never open attachments from an untrusted source; consult HT Technologies first.
- Not use the e-mail systems to store attachments.

Detach and save business related work to the appropriate shared drive/folder.

The automatic forwarding and deletion of e-mails is not allowed.

Internet Access - Statement

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet: Staff

- Staff should preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that should have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- It is illegal to copy or distribute School software or illegal software from other sources.

Internet Use: Staff

It is at the Headteachers discretion on what internet activities are permissible for staff and how this is disseminated.

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Staff must not reveal names of colleagues, customers or clients or any other confidential information acquired through their job on any social networking site or blog.
- Staff are aware that School based email and internet activity can be monitored and explored further if required.
- The School uses management control tools for controlling and monitoring workstations.
- If staff discover an unsuitable site, the website must be closed and the incident reported immediately to the Designated Safeguarding Lead.
- It is the responsibility of the School, by delegation to the HT Technologies, to ensure that Anti-virus protection is installed and kept up to date on all School machines.
- Staff are not permitted to download programs or files on School based equipment.
- If there are any issues related to viruses or anti-virus software, HT Technologies should be informed.

Internet Use: Children

Children are:

- Advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests)

- Advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Encouraged to be wary about publishing specific and detailed private thoughts online.
- Asked to report any incidents of cyberbullying to the School.
- Aware that School based email and internet activity can be monitored and explored further if required.
- Pupils are not permitted to download programs or files on School based equipment.
- If pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the teacher and recorded on the E-Safety Incident Form.

Data storage and processing

Staff and pupils are expected to save all data relating to their work to their School laptop/ PC or to the School's central server. Staff devices should be password / PIN protected if any data or passwords are stored on them. No personal data of staff or pupils should be stored on personal memory sticks. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the E-Safety co-ordinator or Headteacher.

Password security

Staff Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks, including the Management Information System.

All staff:

- Must read and sign an Acceptable Use Agreement to demonstrate that they have understood the School's ICT/E-Safety Policy.
- Are provided with an individual network, email and ScholarPack log-in and password.
- Must enter their personal passwords each time they logon. Do not include passwords in any automated logon procedures.
- Must change passwords whenever there is any indication of possible system or password compromise
- Must not record passwords or encryption keys on paper or in an unprotected file.
- Should ensure that all personal passwords that have been disclosed are changed once the requirement is finished. User ID and passwords for staff and pupils who have left the School are removed from the system as soon as is practicable.

Remote Access

Staff are responsible for all activity when using a remote access facility. They should treat the workplace as if they are at work. They must only use equipment with an appropriate level of security for remote access. Staff should ensure that they have appropriate security in place. To prevent unauthorised access to School systems, staff must keep all access information such as logon IDs confidential and must not disclose them to anyone. Staff must avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify it. School information and data must be protected at all times, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-School environment.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents are welcome to take videos and digital images of their children at School events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims but must follow this policy and the Acceptable Use Agreement concerning the sharing, distribution and publication of those images. Those images must only be taken on School equipment: personal equipment must not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before images of pupils are published on the School website.

Images published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Video Calls/Conferencing

The school may from time to time need to utilise video calls or video conferencing. In such instances the following will happen:

- Permission will be sought from parents if their children are involved in video calls or conferencing.

- Permission will be sought from parents if their children are involved in video conferences with endpoints outside of the School.
- All children are supervised when participating in video calls/conferencing.
- All children are supervised by a member of staff when video conferencing with endpoints beyond the School.
- One to one video/voice calls are supervised by a parent when children are learning remotely.
- Approval from the Headteacher is sought prior to all video calls/conferencing in School.
- All School conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conferences is recorded in any medium without the written consent of those taking part.
- Misuse of the webcam by any member of the School community will result in sanctions.

Social Media - Protecting Professional Identity

The school has a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- By providing training, including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- By clearly reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff will ensure that:

- No reference will be made in social media to the children, parents/carers or school staff.
- They will not engage in online discussion of personal matters relating to members of the school community.
- Personal opinions will not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's Social Media accounts:

- The Bursar and Headteacher has access to the school social media account.
- The Head Teacher and Office Manager are responsible for monitoring and administration of these accounts.
- The SMT will deal with any cases of abuse and misuse on a case by case basis.
- Any abuse or misuse will be reported and dealt with on a case by case basis. Incidents will be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly

The 4 'C's Content, Contact, Conduct and Commerce

As stated in KCSIE Sept 2023 - *The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:*

- **Content -** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact -** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct -** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce -** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group - https://apwg.org/

Dealing with unsuitable/inappropriate activities

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use, social media risks, checking of settings, data protection, reporting issues during staff meetings.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- No reference should be made in social media to pupils, parents or carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Geotagging in instant social media posts are discouraged

Cyber Bullying and Prejudice Based Bullying

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. Maldon Court Preparatory School has a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy.

These include:

- No access to public chatrooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) is given
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support pupils and their families.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

A helpful link for parents with regards to cyberbullying Cyberbullying DfE

Peer on Peer Abuse

We recognise that children can abuse their peers online and our staff are clear about the school's policy and procedures regarding peer on peer abuse. All peer on peer abuse is

unacceptable and will be taken seriously. We also recognise that abuse can still occur during a school closure or partial closure and between those children who do attend the school site during these times.
Our staff will remain vigilant to the signs of peer-on-peer abuse and will follow the process set out in our Safeguarding Child Protection Policy

Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect pupils against this risk.

These include:

- No access to public chatrooms, Instant Messaging services and bulletin boards. No mobile phones.
- All online access and pupil generated content in school is monitored and password protected.
- Pupils are taught how to behave responsibly online and how to protect personal information.

Misuse

Maldon Court will not tolerate illegal activities or activities that are inappropriate in a School context and will report illegal activity to the police and/or the Local Authority Designated Officer (LADO). Incidents of misuse or suspected misuse will be dealt with in accordance with the School's Safeguarding Policy.

The School will impose a range of sanctions on any pupil who misuses technology to cyberbully, harass or abuse another pupil in line with our Anti-Bullying Policy.

E-Safety incidents

Incidents of or concerns around E-Safety will be recorded using the E-Safety Incident Form and handed to the Designated Safeguarding Lead.

Complaints

As with all issues of safety at Maldon Court, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to E-Safety, prompt action will be taken to deal with it. Complaints should be addressed to the Headteacher, who will liaise with the E-Safety Coordinator and undertake an investigation where appropriate. The School's Complaints Procedure is available on our website.

This policy has been written in accordance with:

Teaching online safety in schools – June 2019
Preventing and Tackling Bullying – July 2017
UKCIS – Education for a Connected World
National Online Safety - NOC
www.saferinternet.org.uk

Appendices:

- Incident report form
- Responding to incidents of misuse – flowchart
- Admissions form - Pupil Acceptable Use Policy Agreement
- Staff and Volunteers Acceptable Use Policy Agreement

Appendices

MALDON COURT
PREPARATORY SCHOOL

Incident Report Form – (including e-Safety and Bullying) All incidents should be reported to the Designated Safeguarding Lead.

Date:

Name of person reporting incident:

Pupil(s) involved:

Location of incident

In school (please specify):

Outside of school (please specify):

Type of concern:

Cyber bullying harassment	Bullying	Deliberately bypassing security	Accessing unsuitable content	Racist, sexist or homophobic material	Radicalisation or extremism	Material of a sexual nature

Other (please specify):

Nature of incident:

Deliberate access: The material was:

Created	Viewed	Printed	Shown to others	Transmitted to others	Distributed

Accidental access:

The material was:

Created	Viewed	Printed	Shown to others	Transmitted to others	Distributed

Description of incident:

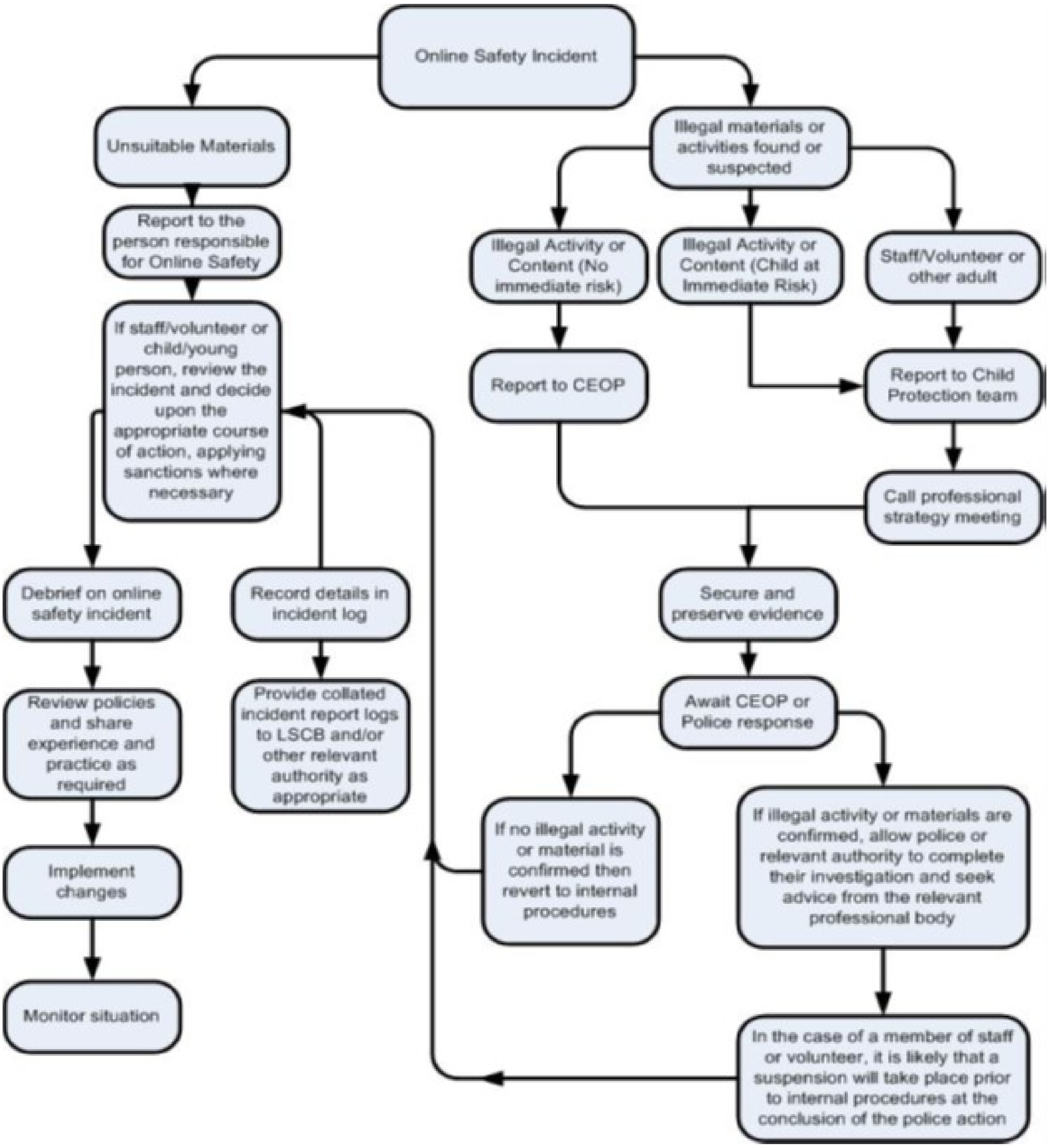
Action taken:

Discussion with child	Reported to Headteacher	Parents informed	Safeguarding referral	Police informed

Details of Action Taken:

Signed DSL ___________________________ Date____________________________

Flowchart for reporting incidences


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

PERMISSION EXPLANATIONS

OFF SITE ACTIVITIES

Permission for your child to leave the school site from time to time during the academic year for local curriculum visits, such as sporting activities, local walks and visits to other local schools. Your child may travel to these events in the school mini-bus or by coach.

PUPIL ACCEPTABLE USE AGREEMENT & E-SAFETY RULES

Computing and ICT (Information and Communication Technology) including the internet, email and mobile technologies etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any form of technology. Please read and discuss the e-Safety rules below with your child. If you have any concerns or would like some explanation, please contact the Computing and E-Safety Coordinator.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- ✓ I will not give out my own details, such as my name, phone number or home address.
- ✓ I will never arrange to meet someone by myself. If I need to meet with someone, I will ask my parents or teacher to arrange the meeting for me and make sure that a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

PERMISSION FOR RECORDED IMAGES – PHOTO AND VIDEO

Permission for recorded images (photographs and videos) to be taken during school activities, including functions and events to support the learning such as trips, school productions, sporting and fun events and Sports Day

Staff Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of Computing in their everyday work.

The school will try to ensure that staff and volunteers will have good access to Computing to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school Computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the Computing systems and other users. I recognise the value of the use of computers for enhancing learning and will ensure that pupils receive opportunities to gain from the use of computers. I will, where possible, educate the young people in my care in the safe use of computers and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the I.C.T systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, parent mail,) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school devices are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will not create WhatsApp groups where children or staff are discussed in an inappropriate manner.

I will be professional in my communications and actions when using school computing systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website, newsletter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils, parents and carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.
- When I use my mobile devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses)
- I will ensure that my data is regularly backed up, in accordance with the relevant school policies.
- I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the school policies or by the school administrators.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school computing equipment in school, but also applies to my use of school computing systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Board of Visitors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name______________________________

Signed____

Date____