Malden Oaks
School & Tuition service

Making the MOST of everyday

Online Safety Policy

Status	Statutory
Review Frequency	Annual
Last Reviewed	Autumn 2026
Next Review Due	Autumn 2027
Responsible for review	DSL
Approval by	Management Committee

In developing and reviewing this policy, the school has had regard to the following legislation and guidance, together with other relevant considerations:

Legislation	Education Act 1996 (as amended) Education and Inspections Act 2006 Children's Wellbeing and Schools Act 2026 Equality Act 2010. Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.
Official Guidance	Keeping Children Safe in Education • Teaching online safety • Meeting digital and technology standards • Preventing and tackling bullying • Relationships and sex education (RSE) and health education • Searching, screening and confiscation • Mobile phones in schools

Contents

Introduction **2**

1. Aims

Malden Oaks aims to:

- Have robust processes in place to ensure the online safety of students, staff and Management Committee Members
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

<u>The 4 key categories of risk</u>

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), including those generated using AI, and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the statutory safeguarding guidance, Keeping Children Safe in Education from the Department for Education (DfE) and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation
- Mobile phones in schools

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Management Committee

The Management Committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Management Committee will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

The Management Committee will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Management Committee will also make sure all staff receive regular online safety updates (via whole school briefing, 'Safeguarding Segments' and the weekly update), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Management Committee will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Management Committee will make sure that the school teaches students how to keep themselves and others safe, including online.

The Management Committee will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The management committee will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The Management Committee Member who oversees online safety is Stuart Holmes, the safeguarding link.

All Management Committee members will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach will often be more suitable

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances - to ensure all safeguarding practices continue running effectively.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and Management Committee to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing the Management Committee with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT Manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Management Committee
- Undertaking annual risk assessments that consider and reflect the risks students face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The Heads of School, who are all DDSLs lead on:

- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring as advised by the DSL
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy which is called Relationships & Communication Policy

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and making sure that students follow the school's terms on acceptable use (Appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking with the HOS at their provision
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes by logging an ICT Request
- Discussing and logging any online safety incidents with their HOS and CPOMS if they are advised to.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school Relationship & Communication Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify their child's Head of School of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

Further information can be found on the school's website

3.7 Visitors

Visitors who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

4.1 students will be taught about online safety as part of the curriculum

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026).

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In KS3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, students will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. students should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and/or may post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Students should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Students should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Students should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Students should be taught where to go for advice and support about something they have seen online. Students should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice

- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect students who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

4.2 students will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All students will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack

- How to report a personal data breach

students will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy named Relationships & Communication Policy.)

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 10 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy, named the Relationships & Communication Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL/DDSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.3 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Malden Oaks recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or ‘deep nudes’, where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone’s likeness.

Malden Oaks will treat any use of AI to bully students very seriously, in line with our Relationships & Communications Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by Malden Oaks, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff. Further information can be found in our AI Policy

6. Acceptable use of the internet in school

All students, parents/carers, staff and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet HOS will decide which is most appropriate for the student given their age and understanding. Visitors will be expected to read and agree to the school’s terms on acceptable use, if relevant. Copies of the documents can be found here.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by students, staff, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

7. Students using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Students are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by their Head of School.

Where there is an arrangement by exception, any use of mobile devices in school by students must be in line with the acceptable use agreement.

Our post 16 students in 6Oaks are permitted access to their mobile phone at certain limited times and locations (e.g. in the 6 Oaks common room outside of lessons). They are not given the wifi password.

8. Staff Use of Devices

Staff using work devices outside school

Staff may be given a chrome book to complete work offsite. These staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager via an ICT Request.

Staff using personal devices for work purposes

If staff use personal devices, such as their phone or a personal computer, to access their Malden Oaks Google Account, they are reminded of the following:

- Their Malden Oaks account must only be accessible to them – so all the same precautions and security settings must be active as on a work device (see above)
- Their hard drive should be encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Up to date anti-malware should be installed
- Operating systems should be kept up to date by promptly installing the latest updates
- WhatsApp should not be used to discuss student information or for any other work related purposes. Google Chat should be used for this instead.

9. How the school will respond to issues of misuse

The action taken if a student misuses the school's ICT systems or internet will depend on the individual circumstances, nature and seriousness of the specific incident, and will always prioritise all student's safety and development..

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct/ Disciplinary Policy, depending

on its nature. . The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training for staff & Management Committee

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, whole staff briefings and Weekly Updates.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, including images generated or altered by AI, especially around chat groups
- Sharing of abusive images and pornography, including images generated or altered by AI, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLS will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

The Management Committee will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DDSLs log safeguarding issues related to online safety on CPOMS.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the Management Committee. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Relationships & Communication (Behaviour) policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile phones policy
- AI policy

Appendix 1: acceptable use agreement (staff, Management Committee & and visitors)

Name of staff member/MC Member/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable),	
I will: • Only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let my HOS or another DDSL know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too. • I will ensure that when I am working with a student who is using a chrome book or other device, I will be able to see the student's screen • I will use generative AI in line with the school's AI policy.	I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms unless I am responsible for my school's Instagram account or am a DSL/DDSL with oversight of this. Further guidance on the use of Instagram can be found here • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Input, upload, or process any personal data of students, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times • Share my password with others or log in to the school's network using someone else's details • Take photographs of students that show their face or other identifying features. Any photos taken should be deleted from the device the same day, once the photo has been saved in the student's area/ uploaded to Instagram.

	• Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
Signed:	Date:

Appendix 2: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Are there any areas of online safety in which you would like training/further training?	