Malden Oaks
School & Tuition service

Making the MOST of every day

# Online Safety Policy

**Responsible:** Senior Deputy Head/ Management Committee

**Status:** Statutory

**Date reviewed:** Sept 2025

**Next review Date:** Sept 2026

# 1. Introduction

Malden Oaks aims to ensure that students, staff, and other members of our community are able to work online and use the internet safely. This policy, together with our Safeguarding Policy, sets out our approach to online safety.

Our approach to online safety is based on the **4 key categories of risk**
(also known as the **4 Cs**):

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, 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** – personal 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), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

# 2. Roles & Responsibilities

## 2.1. 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

- 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.
- make sure all staff receive regular online safety updates (via email, briefings, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- 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).
- make sure that the school teaches pupils how to keep themselves and others safe, including online.
- make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. 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

All members of the management committee 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 2)
- 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 pupils 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 may often be more suitable

### 2.2. Headteacher & Heads of School

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

Heads of School are responsible to the Headteacher for making sure that staff within their provision understand this policy, and for implementing the policy within their provision.

### 2.3. Designated Safeguarding Lead (DSL)

The details of the school's DSL and deputies are set out in the Safeguarding Policy.

The DSL has lead responsibility for online safety at Malden Oaks, in particular:

- Supporting the Headteacher and Heads of School 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, Heads of School, ICT manager, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Safeguarding Policy
- Responding to safeguarding concerns identified by filtering and monitoring
- 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 any other bullying incident.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher, Heads of School, and/or management committee
- Undertaking annual risk assessments that consider and reflect the risks pupils 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

(this list is not exhaustive)

### 2.4. 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 pupils

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
- 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 dealt with appropriately in line with the school behaviour policy

(this list is not exhaustive)

### 2.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Reading this policy, and asking any questions they may have to ensure that they understand it
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and making sure that pupils 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 flagging it with their Head of School.
- Following the correct procedures by using their own LGfL login if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL and deputies to make 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 dealt with appropriately in line with the school's ethos and approach
- 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 exhaustive)

### 2.6. Parents & Carers

Parents/carers are expected to:

- Notify a member of staff 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 (appendix 1)

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

### 2.7. Visitors

Visitors and members of the community 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 2).

# 3. Key Issues in Online Safety

## 3.1. Email, Messaging, and Commenting Systems

All staff and students are provided with an @maldenoaks.rbksch.org account which will allow them access to these systems.

### 3.1.1. Emails

Staff should use their school email address for all school-related email communications. It is not appropriate for staff to use personal accounts, or accounts provided by other businesses/charities/etc. for any work-related purposes.

Students are also expected to use their school account when communicating with staff. Staff should only contact a student on a personal address where this has been agreed with the Head of School.

Emails may be sent to students/parents through EduLink. This is a one-way communication system, and so messages expecting a response should include a school email address. If EduLink is not used, then the email addresses must be checked against the details on EduLink before sending, even if the email has been used before, or a response is being sent to a message that appears to be from the student/parent concerned.

### 3.1.2. Text messaging

Text messages may be sent to students/parents through EduLink. This is a one-way communication system, and so messages expecting a response should include a school email address or phone number.

Text messages to students and parents may also be sent from a school device, but only with the permission of the relevant Head of School. The number must be checked against the details on EduLink before sending, even if the number has been used before, or a response is being sent to a message that appears to be from the student/parent concerned.

### 3.1.3. Phone calls

Phone calls to students/parents may be made from any Malden Oaks device.

Calls may also be made from a personal device, but only by withholding the number (dial "141" before the number). It is not appropriate for staff to allow parents or students to know their personal phone number.

Numbers must be checked against those on EduLink before making a call, even if a call has been made to that number before. Staff should not save parent or student numbers as contacts on any device - they should always get the number from EduLink.

When answering a call, staff should verify that the incoming call number matches the number on EduLink before confirming any information about a student (including whether or not they are actually a student at the school).

## 3.2. Social Media

### 3.2.1. Definition of Social Media

Social media platforms are online services which allow users to share personal or professional updates, images, videos, etc. Commonly-used social media platforms include Facebook, Twitter/X, Instagram, TikTok, and similar.

More broadly, social media also includes online apps and gaming such as dating apps, multiplayer games, etc.

### 3.2.2. Official School Social Media

Malden Oaks currently has the following official social media accounts:

| Platform | Handle & Link |
|---|---|
| Instagram | @lowerschoolkingston<br>@moupperschool<br>@60aksmaldenoaks<br>@maldenoakskingstontuition<br>@richmondtuitionmo<br>@mo_discover |

The DDSLs in each provision are responsible for overseeing the management of any social media accounts associated with their provision. New accounts should only be created with the approval of the Head of School.

If any new social media accounts are created, these should be reported to the DSL immediately for inclusion in the list above.

Official social media accounts should not allow for public comments or messages to be sent. Where messaging functionality cannot be disabled, the account should clearly explain that messages will not be responded to.

### 3.2.3. Staff accounts

Staff should ensure that their personal social media accounts are kept private and that content is only visible to verified "friends".

Any public social media accounts should be kept appropriate, on the basis that students are likely to find and attempt to follow them.

Teaching and Leadership staff are reminded that they have professional duties under the Teachers' Standards, and that there have been a number of Teacher Regulation Agency cases that have resulted in teachers being prohibited from teaching as a result of inappropriate use of social media.

### 3.2.4. Social Media Age Limits

Many social media platforms have minimum age limits (often 13 years old). However, these are generally not strictly enforced, and we are aware that many children may access them at a younger age.

In line with our usual approach, we focus on supporting students with issues they encounter in online spaces, rather than attempting to punish or police their use of social media. Where there are safeguarding concerns relating to a student's use of social media, these will be handled through our usual safeguarding procedures.

### 3.2.5. Online Reputation

There is often discussion about schools online, particularly on social media and online "reviews" of the school.

Where staff see discussion of the school, whether positive or negative, they should **not** engage with this. If there are concerns about what is being discussed, these should be reported through the usual safeguarding procedures (if safeguarding-related) or to their line manager (for more general concerns).

Parents with concerns or complaints about the school should contact us by email to discuss the matter in private. A copy of our complaints procedure is available on request. Sharing complaints online is unlikely to resolve the matter, but may cause upset to staff, students, and parents.

### 3.2.6. Staff-student interactions

It is not appropriate for staff and students to be "friends" (or equivalent) on any social media platform. The only exception to this is where there are pre-existing family links, but this must be declared by the staff member as soon as they become aware, and approved by the Headteacher.

A staff member attempting to:

- follow or be "friends" with a student
- contact students through social media
- encourage a student to follow or be "friends" with them on social media

is a serious breach of professional boundaries. Even if accidental, incidents such as these must be reported to the Headteacher immediately.

A student attempting to follow or be "friends" with a member of staff's personal account should be reported to a Safeguarding Lead as soon as possible. The staff member should explain to the student the reason for professional boundaries and appropriate interaction.

### 3.2.7. Former students over the age of 18

While staff are not strictly forbidden from interacting with former students that have left the school and are over the age of 18, they should be aware that the vulnerable nature of most of our students means that this is generally highly inappropriate and may constitute a breach of their professional duties. Staff should seek advice from a DSL if they have any concerns about interactions with former students.

## 3.3. Use of own devices

### 3.3.1. Students

Students in some provisions may be required to hand in their phones at reception. Phones may also need to be handed in where this is agreed as part of the student's individual support needs.

Where students do bring their phones into school, they should normally only be used outside of lessons, and in accordance with our Acceptable Use Policy.

Students should only use mobile phones in lessons where the teacher has given explicit permission as part of a teaching & learning activity. Students should not take photos or videos of other students or staff.

Students should not bring any other devices into school unless agreed with the Head of School (for example, 6th Form students may wish to bring tablets in for use in study periods).

### 3.3.2. Staff

Staff may bring personal devices into work if they wish, but remain responsible for the safety and security of their own devices.

Devices should be kept password-protected, and should be locked if left unattended.

More information is available in the Acceptable Use Policy.

## 3.4. Digital images & video

The use of images of students is subject to our Data Protection Policy, and the relevant consents given by parents/students/staff when they join the school.

### 3.4.1. Taking Photos/Videos

Wherever possible, photos and videos will be taken using school devices.

With the permission of the relevant Head of School, a personal device may be used to take photos/videos. However, these must be transferred to a Malden Oaks device or storage system as soon as possible, and then deleted from the personal device (note that many phones automatically back-up photos and so back-ups may also need to be deleted).

### 3.4.2. Using Photos/Videos for publicity (including displays)

Staff are reminded that some of our students are particularly vulnerable, and there may be dangers associated with sharing images or videos of them online (e.g. looked-after children whose location is not disclosed to their birth parents).

When photos/videos of students are taken, staff should check the permissions on EduLink before using them. Staff should remember that parents do not have an unrestricted right to exercise their child's data rights. Therefore, staff should usually seek the **student's** consent before sharing photos/videos publicly, even if parental consent has already been given.

Photos or videos used in public materials should never identify students with more than a first name.

### 3.4.3. Using Photos/Videos for assessment & teaching purposes

Permission is not usually needed when photos or videos are taken for assessment or teaching purposes, but staff should check with their Head of School if they are unsure.

## 3.5. Artificial Intelligence (AI)

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

### 3.5.1. Inappropriate use of AI tools

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used in inappropriate ways. For example, in the form of 'deepfakes', 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).

We treat any use of AI in inappropriate ways very seriously, in line with our behaviour policy and Safeguarding & Child Protection Policy.

### 3.5.2. Staff use of AI tools

Staff should be cautious of using AI tools either for themselves or as part of the curriculum. In particular, staff should be aware that:

- AI cannot be trusted to produce reliable factual information – all information provided by AI tools should be verified against an objective human-written source.
- While AI can be a useful skill to assist with some basic research, drafting documents, notes, etc., overreliance on it can prevent students from acquiring critical thinking and writing skills.
- Some AI tools can reproduce text that is entered into them by other users – for this reason, staff must **not** enter personal information of students or staff into AI tools.

Where staff use AI tools to assist with writing review notes, reports, etc., they **must** fully proofread these to ensure they are accurate.

# 4. Prevention & Awareness

## 4.1. Education & Curriculum

Pupils will be taught about online safety as part of the curriculum. Both the National Curriculum for computing, and the statutory guidance on Relationships Education, Relationships and Sex Education and Health Education (RSHE) include relevant content. The box below sets out the requirements for students to learn.

Although the National Curriculum does not apply to Malden Oaks, we aim to ensure that all students have the best learning opportunities and experience possible, which will include most of the same content.

As with all of our teaching, the content and delivery will be tailored to each individual student, taking into account any SEND or other needs. Some students may require further consolidation of the primary school curriculum content in addition to the secondary content. Teachers will also be sensitive to the needs of children at risk, particularly those who have been victims of abuse, when teaching about safeguarding.

**National Curriculum Requirements**
In **KS3**, pupils 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

In **KS4**, pupils 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

**RSHE Requirements (until 31 August 2026)**
By the end of secondary school, pupils should know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail

- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

*New RSHE guidance comes into effect from 1 September 2026. For awareness, the new requirements are set out below.*

**RHSE Requirements (from 1 September 2026)**

- 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils 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. Pupils should be taught where to go for advice and support about something they have seen online. Pupils 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 pupils 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

## 4.2. Filtering & Monitoring Systems

### 4.2.1. Dukes Centre (Upper School, 6 Oaks, and Business Services) and Surbiton site (Lower School)

There are filtering and monitoring systems in place on the school networks and WiFi at these locations. Staff should not rely on these however, and should ensure that they help support and guide students' use of the internet in lessons.

If staff believe that a website is being incorrectly blocked, or that an unblocked website should be blocked, they should contact the DSL.

Staff may use their LGfL login to bypass the filter where necessary for teaching & learning purposes. This must only be done on a staff device and under no circumstances may a student be informed of staff login details.

### 4.2.2. Craigie Building (Kingston Tuition)

The filtering and monitoring system is managed by St John the Baptist CofE Junior School. Details of their filtering and monitoring arrangements are available from their website.

### 4.2.3. All other locations (including home & community tuition)

There are no school filtering or monitoring systems in place at these locations. Students should only use the internet when under direct supervision by a member of staff

## 4.3. Training

All new staff members will receive training, as part of their onboarding, 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, e-bulletins and staff meetings).

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, especially around chat groups
    - Sharing of abusive images and pornography, 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

# 5. Responding to Incidents

## 5.1. Safeguarding Concerns & Incidents

Any concerns or issues should be reported through the usual Safeguarding processes.

## 5.2. Misuse of IT

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

The school will consider what the appropriate support in relation to incidents that involve illegal activity or content, or otherwise serious incidents.

# 6. Legislation & Guidance

This policy includes content based on the following guidance from the Department for Education:

Statutory Guidance

- Keeping Children Safe in Education
- Relationships and sex education (RSE) and health education
- National curriculum in England: computing programmes of study

Non-Statutory Guidance

- Teaching online safety in schools
- Preventing bullying
- Searching, screening and confiscation in schools
- The Prevent duty: safeguarding learners vulnerable to radicalisation

This guidance, and this policy, reflects the school's duties and powers under legislation including, but not limited to:

- Education Act 1996
- Education and Inspections Act 2006
- Equality Act 2010

# Appendix 1: ICT Acceptable Use Policy (Students)

**Name of student:**

**Use of School ICT Systems**

I **understand:**

- This agreement applies whenever I use the school's ICT systems (including computers, laptops, and WiFi)
- My use of the ICT systems will be monitored – teachers can see what you are using the systems for

I **will**:

- Use the ICT systems for educational purposes only
- Only use the ICT systems with a teacher's permission
- Always log out of my account when I am finished with it
- Use appropriate language when communicating online
- Tell a teacher or my parent/carer immediately if I find anything that might upset, distress, or harm me or anyone else
- Consult my parent/carer or a teacher before agreeing to meet anyone in person that I met online

I will **not**

- Share my username or password with anyone else
- Use anyone else's username or password
- Share any personal details (e.g. name, address, phone number) online without checking with a teacher or my parent/carer first
- Open any email attachments or links without checking with a teacher first
- Create, link to, or share anything offensive, pornographic, or otherwise inappropriate
- Attempt to bypass the school's monitoring or filtering systems

**Personal Devices (mobile phones, tablets, smart watches, etc.)**

I **will**:

- Get permission before bringing any device (other than a phone) into school
- If requested, hand my phone/device in at reception and/or to a teacher. I understand it will be looked after and returned at the end of the school day.
- Use any phone/device appropriately and responsibly, in line with the policy above on the use of the school ICT systems

I will **not**:

- Use my phone/device in lessons unless the teacher has given permission

I agree to follow the policy above, and to check with a teacher if I have any questions or am unsure about anything.

| | |
|---|---|
| **Signed (student):** | **Date:** |

I agree for my child to use the school's ICT systems and internet when appropriately supervised. I will ensure that my child understands and follows the policy above.

| | |
|---|---|
| **Signed (parent/carer):** | **Date:** |

# Appendix 2: ICT Acceptable Use Policy (Staff, MC members, volunteers, visitors)

**Name:**

I **understand:**

- This agreement applies whenever I use the school's ICT systems (including computers, laptops, and WiFi)
- My use of the ICT systems will be monitored

I **will**:

- Follow all school policies, including the Online Safety Policy, Safeguarding & Child Protection Policy, and the Staff Code of Conduct.
- Seek advice and/or training if I am unsure on how to use the school's ICT systems effectively or safely
- Keep my login details secure and not share them with anyone, including other school staff
- Supervise students' use of the school's ICT systems in line with the Acceptable Use Policy for students, and support students to use ICT systems appropriately
- Promptly inform the DSL (or a deputy) of any safeguarding concerns relating to students' use of the school's ICT systems
- Promptly inform the Headteacher of any low level or other concerns relating to my, or other adults', use of the school's ICT systems (or the Chair of the Management Committee where my concerns are about the Headteacher)
- Take all reasonable steps to ensure that work devices (and any personal device with access to a work account) are kept secure and password-protected.
- Immediately inform the ICT manager and my line manager if a school device (or any personal device with access to a work account) is lost or stolen.

I **will not**:

- Use the school's ICT systems to access, or attempt to access, anything inappropriate for a school setting
- Install any unauthorised software, or connect any unauthorised hardware or devices to the school network.
- Use anybody else's login details to access the school's ICT systems
- Access, modify, or share (or attempt to) any data or information without authorisation
- Take any photos or videos of students unless it is for educational purposes and the photos/videos are promptly transferred to the school system and deleted from any personal device

**Signed:**

**Date:**