Online Safety Policy

Responsible Person	Amanda Woolcombe, Headteacher
Dated	September 2026
Date of next review	September 2027

Contents

Introduction

Aims

Legislation and guidance

Roles and responsibilities

Educating pupils about online safety

Educating parent/carers about online safety

Cyber-bullying

Acceptable use of the internet in school

Pupils using mobile devices in school

Staff using work devices outside school

How the school will respond to issues of misuse

Training

Monitoring arrangements

Links with other policies

Appendices

1. EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)
2. KS2 Acceptable Use Agreement (pupils and parents/carers)
3. Acceptable Use Agreement (staff, governors, volunteers and visitors)
4, Online safety training needs (self-audit for staff)
5. Online safety incident report log
6. Useful Links for Educational Settings
7. Rules for Internet Use Poster
8. Consent Form for Taking and Using Photographs
9. Code of Practice for the Use of Images Online
10. Children, ICT & Online Safety – Information Leaflet
11. Online Safety Audit Form

Introduction

It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. Madginford Primary School recognises that online safety is an essential part of safeguarding and will adopt a whole school approach to online safety which empowers, protects, and educates pupils and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Online safety is considered a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL, and parental engagement.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils 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

The 4 key categories of risk

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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **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 them 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 including those generated by AI (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

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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 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 pupils' 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.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins 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.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 their safeguarding needs.

The governor who oversees online safety is: the Chair of Governors, Mr Toby Butler

All governors will:

- Ensure 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)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

- Ensure 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

The headteacher

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

The designated safeguarding leads

Details of the school's designated safeguarding leads (DSL) and the team of deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure 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
- 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
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 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 governing board
- Undertaking annual risk assessments that consider and reflect the risks children 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 intended to be exhaustive.)

The ICT support provider

The ICT support provider 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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring 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
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

(This list is not intended to be exhaustive.)

All staff and volunteers

All staff, including contractors and agency staff, and volunteers 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 (Appendix 3), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1 & 2)
- 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 following the school's safeguarding procedures.
- Following the correct procedures by informing the DSL and headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour 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.)

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)

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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

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

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

- The text below is taken from the National Curriculum computing programmes of study.
- It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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 pupils with SEND.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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.)

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes. 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL 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.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable.

If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (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 Bard.

Madginford Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Madginford Primary school will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Madginford Primary School recognises that generative artificial intelligence (AI) tools can support teaching, learning, communication and administrative tasks when used safely, lawfully and appropriately. However, AI can also create safeguarding, data protection, privacy, intellectual property, academic integrity and information security risks. These include, but are not limited to:

- exposure to inappropriate or harmful content, including bullying, harassment, abuse and exploitation
- the creation or sharing of AI-generated or digitally manipulated images
- privacy and data protection breaches/risks
- intellectual property infringements
- academic integrity challenges such as plagiarism and cheating
- exposure to inaccurate, misleading, or biased content.

Settings should make clear decisions about whether, when, and how AI tools may be used by staff and by children.

Any use of AI should be risk assessed, aligned with data protection laws and safeguarding expectations, and limited to tools that have been approved by leaders. This includes AI tools that record, transcribe, summarise or generate notes from meetings, lessons, training or online discussions.

Participants should be made aware when such tools are being used, what information will be captured, how it will be used and stored, and who will have access to it.

Staff and learners should be clear that AI must not replace professional judgement, safeguarding decision-making, assessment decisions or direct support from safe adults.

The DfE's data protection guidance for schools says generative AI use needs to be carefully planned and that schools should check with their DPO or IT lead for further guidance about what is acceptable to use.
The following links may also provide further information for leaders to consider:

- Generative artificial intelligence (AI) in education - GOV.UK
- Using AI in education settings: support materials - GOV.UK
- Generative Artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK
- Artificial Intelligence and Online Safety | SWGfL
- Using artificial intelligence (AI) safely | Internet Matters
- A Safeguarding First Approach to adopting Gen-AI in schools | LGFL

Madginford Primary School will maintain a record of any generative AI tools approved for staff and/or pupils.

Madginford Primary School recognises that the use of images online, including through AI tools, can create safeguarding, privacy and data protection risks for children and staff. Images of pupils or staff must not be uploaded to, generated by, edited in, or shared through AI tools unless risk assessed and approved by the school. Any taking or publishing of images of pupils or staff will always be in line with our image use, consent, acceptable use, data protection and safeguarding arrangements.

Madginford Primary School will ensure expectations about the safe and appropriate use of AI are set out in our acceptable use arrangements.

Madginford Primary School will respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour, data protection, complaints, allegations against staff and child protection.

Concerns involving AI-generated or digitally manipulated content, including nude or semi-nude imagery, harmful impersonation, bullying, harassment, abuse or exploitation, will be reported to the DSL and responded to in line with this policy.

Where the school believe that AI tools may have facilitated the creation of Child Sexual Abuse Material (CSAM), the school will respond in line with this policy, local safeguarding procedures, the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and national guidance from the IWF and NCA-CEOP as appropriate.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 3.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- School time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices 1 and 2). Pupils will not have access to mobile phones during the school day, including during lessons, breaktimes and lunchtimes. Any exceptions will be determined by the school leadership in line with safeguarding policies.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Madginford Primary School recognises the safeguarding risks that can be posed by mobile phones, smart devices and wearable technology. This includes devices that can send or receive messages or notifications, connect to mobile networks or the internet, record images, audio or video, or share location information, and may include but is not limited to, devices with built-in mobile connectivity, smart phones, smart watches, smart glasses, fitness trackers and other wearable technology.

Madginford Primary School recognises that safeguarding concerns involving mobile phones, smart devices and wearable technology may arise outside of school, but still affect children's safety, wellbeing, relationships, attendance or learning. Such concerns will be reported to the DSL and responded to in line with this policy.

Madginford Primary School will ensure that mobile phone and smart technology expectations do not discourage pupils from disclosing safeguarding concerns. Where a pupil needs to report messages, images, videos, posts or other content as part of reporting a concern, staff will respond in line with this policy, avoid viewing or sharing illegal or harmful content unnecessarily, and report the concern to the DSL.

Staff using work devices outside school

All 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is 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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 3.

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 DSL and School's IT Technician.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 disciplinary procedures and staff code of conduct. 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.

Training

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, 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, 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.

Governors 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

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

The governing body has overall strategic responsibility for ensuring that appropriate filtering and monitoring systems and processes are in place as part of the school's wider safeguarding arrangements. This includes ensuring that filtering and monitoring provision is reviewed, that roles and responsibilities are clear, and that leaders and relevant staff understand how to manage systems effectively and escalate safeguarding concerns when identified.

Miss C Allen and Miss L Stamp, members of the senior leadership team, have operational responsibility for filtering and monitoring and will work with the nominated governor representative to ensure there is oversight of the school's approach to meeting the DfE Filtering and monitoring standards.

Our senior leadership team is responsible for:

- ensuring filtering and monitoring systems are appropriate to the [school/college] context and safeguarding risk profile.
- procuring filtering and monitoring systems.
- documenting decisions on what is blocked or allowed and why.
- ensuring reviews and checks are completed and recorded.
- overseeing reports.
- ensuring all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- ensuring the DSL and IT service providers have sufficient time and support to manage their filtering and monitoring responsibilities.

The DSL has lead responsibility for overseeing and acting on:

- any filtering and monitoring reports.
- any child protection or safeguarding concerns identified.
- checks to filtering and monitoring systems.

The IT service providers have technical responsibility for:

- maintaining filtering and monitoring systems.
- providing filtering and monitoring reports.
- completing technical actions identified following any concerns or checks to systems.
- working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

All staff will receive information about filtering and monitoring as part of induction and ongoing safeguarding training. This will include their responsibilities for reporting concerns, responding to incidents, following acceptable use expectations and escalating concerns where filtering or monitoring may not be working effectively.

All staff, pupils and parents/carers are expected to follow this policy, the school's acceptable use policy and to report any filtering or monitoring concerns.

When procuring or making decisions about filtering and monitoring provision, the senior leadership team will work closely with the DSL and the IT service providers to ensure systems are appropriate to the school's needs and circumstances.

Decisions about filtering and monitoring will be informed by the school's safeguarding risk profile. This will include consideration of:

- the age and ability of pupils
- children who may be at greater risk of harm
- how often pupils access technology
- our local context, including contextual safeguarding concerns
- the devices, systems, platforms and networks in use
- remote access arrangements
- any use of Bring Your Own Devices (BYOD)
- the schools's Prevent duty risk assessment
- emerging risks, including mobile platforms, apps, cloud services and generative AI.

Decisions about what is blocked or allowed, and the rationale for those decisions, will be recorded. Any changes to filtering and monitoring arrangements will be assessed by staff with appropriate safeguarding, educational and technical knowledge and approved by the leadership team. Changes will be logged and recorded.

Reviews of filtering and monitoring provision will be carried out at least once every academic year by the senior leadership team member responsible for filtering and monitoring, with support from the DSL and IT Service Providers. Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

- Reviews will consider whether filtering and monitoring remain effective across all relevant devices, systems and locations, including school-owned devices, mobile devices, apps, embedded browsers, cloud services, remote access, guest access and any permitted personal device use.
- Filtering and monitoring arrangements will be reviewed earlier than the annual review where there is a safeguarding concern, a change in technology or working practice, the introduction of new systems or devices, changes to remote access or personal device arrangements, or updates to local or national guidance.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

_____	_____	_____
(Signature)	(Role)	(Date)

Appendix 1

EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2

KS2 Acceptable Use Agreement (pupils and parents/carers)	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3

Acceptable Use Agreement (staff, governors, volunteers and visitors)	
Name of staff member/governor/volunteer/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 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 which could harm the school's reputation • Access social networking sites or chat rooms • 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 • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils 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	
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 the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which 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 pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4

Online safety training needs (self-audit for staff)	
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 pupils can abuse their peers online?	
Do you know what you must do if a pupil 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 pupils 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?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6

Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings:

- onlinesafety@kent.gov.uk
- edsafeguardinghq@kent.gov.uk

Central Team:

- Head of Service: Claire Ray - 03000 423 169
- Training and Development Manager: Rebecca Avery - 03000 423 168
- Senior Safeguarding Advisor: Robin Brivio - 03000 423 169
- Online Safety: Ashley Assiter, Online Safety Development Officer (Monday/Tuesday/Wednesday) - 03000 423 164

Education Safeguarding Advisors:

- Myles O'Keeffe
- Anup Kandola
- Kirstie Owens
- Gemma Lawford
- Gemma Willson (Monday/Tuesday) Claire Ledger (Wednesday/Thursday/Friday)

Education Safeguarding Assistants:

- Joanne Barnett (North/West)
- Vacancy (South/East)

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999.
For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk

    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Appendix 7

Rules for Internet Use Poster



Appendix 8

Consent Form for Taking and Using Photographs

Child's name: _____ Child's Date of Birth: _____

Dear Parents/Carers

At Madginford Primary School we take photographs and film pupils as part of our core activity of education. During your child's time at Madginford Primary School this occurs as part of normal teaching, learning, assessment and safeguarding procedures and as such we do not need your permission for these activities.

However, we do seek your permission to take photographs of your child and use them in the ways described below. Please consider carefully the ramification of not granting permission before you decide.

Please tick all the relevant boxes, sign each item below and return this form to school.

I give consent for my child's photo to be stored in SIMS (School Information Management System) as part of their individual data file.

Yes ☐ No ☐ Signed: _____

I give consent for my child's photograph to be taken by the school photographer, for individual, group, class and whole school photographs.

Yes ☐ No ☐ Signed: _____

I give my consent for photos and videos of my child with their first name to be used on the school website and/or the school's learning platform.

Yes ☐ No ☐ Signed: _____

I give my consent for photos of my child with their first name to be used in classroom, corridor and entrance displays.

Yes ☐ No ☐ Signed: _____

I give my consent for photos and the name of my child to appear in local newspapers and magazines. Please note that some newspapers may require the child's full name and may store photographs for online use.

Yes ☐ No ☐ Signed: _____

I give my consent for my child to be photographed and filmed by staff and fellow parents during school productions and events as long as it is made clear each time that these must only be used for personal viewing purposes and must not be published in any format including on-line.

Yes ☐ No ☐ Signed: _____

I give my consent for my child's image and full name to be used for identification purposes should they have a specific educational, dietary or medical need which needs to be communicated to all staff for safeguarding purposes. (These photographs will be displayed in the medical room, staff room and school kitchen only).

Yes ☐ No ☐ Signed: _____

I give my consent for my child's named image to be taken by the adult in charge on school trips or visits. (The image would only be used in the event of an emergency and is shredded on return to school).

Yes ☐ No ☐ Signed: _____

I give permission to participate in video conferencing. (Occasionally your child's class may talk to other children or an author for example, outside of the school under the supervision of their Class Teacher).

Yes ☐ No ☐ Signed: _____

Please note: this form is valid for the period of time your child is on roll at Madginford Primary School. Where the consent is given for a specific reason e.g. a trip, medical condition etc. once this need ends the image will be destroyed by shredding.

If you wish to make any changes, please email the school office at office@mps.kent.sch.uk, call the school on 01622 734539 or visit in person, and we will supply you with a new form. If you have any questions, please contact the school office.

Why are we asking for your consent again?

You may be aware that there are new data protection rules from 25th May 2018. To ensure Madginford Primary School meets the new requirements, we need to obtain your consent under the new regulations to take and use photos of your child.

We really value using photos your child to showcase what they do in school and demonstrate what school life is like to other stakeholders and the wider community, so we really appreciate you taking the time to give consent again.

Furthermore, it is hugely beneficial to be able to identify children with educational, dietary or medical needs to all staff, to safeguard and ensure their well-being.



Mrs Amanda Woolcombe
Headteacher

Parent or carer's signature: _____

Date: _____

Relationship to named child: _____

Appendix 9

Code of Practice for the Use of Images Online

The Photograph Consent Form is valid for the time your child attends Madginford Primary School. We will only include the first name of children in photographs which are published in the school prospectus, newsletter, website or around the school. This may include group or class images with general labels, such as "a literacy lesson" or "making biscuits". Only images of children who are suitable dressed will be used, i.e. wearing full school uniform or P.E. T-shirt and shorts.

We will contact you if your child is photographed for publication in the local press and to obtain consent for that photograph to be printed using the child's first name only. Personal information for a child/family will never be used, e.g. home address or telephone number.

Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends; family events, holidays and school events are moments we all like to capture in photos or on video. With social media we have the ability to add images/videos to our online social network, such as Facebook, YouTube and many others. This means that we can easily share our photos and video with family and friends. Whilst this can be very useful to all of us at home, in schools and educational settings we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

What should we all think about before adding any images or video online and are there any risks?

- Once posted and shared online any image/video can be copied and will stay online forever.
- Some children are at risk and MUST NOT have their image put online and not all members of the school community will know who they are.
- Some people do not want their images online for personal/religious reasons.
- Some children and staff may have a complex family background which means that sharing their image online can have unforeseen consequences.
- Therefore, in order to keep all members of the school community safe we must all 'Think Before We Post' online

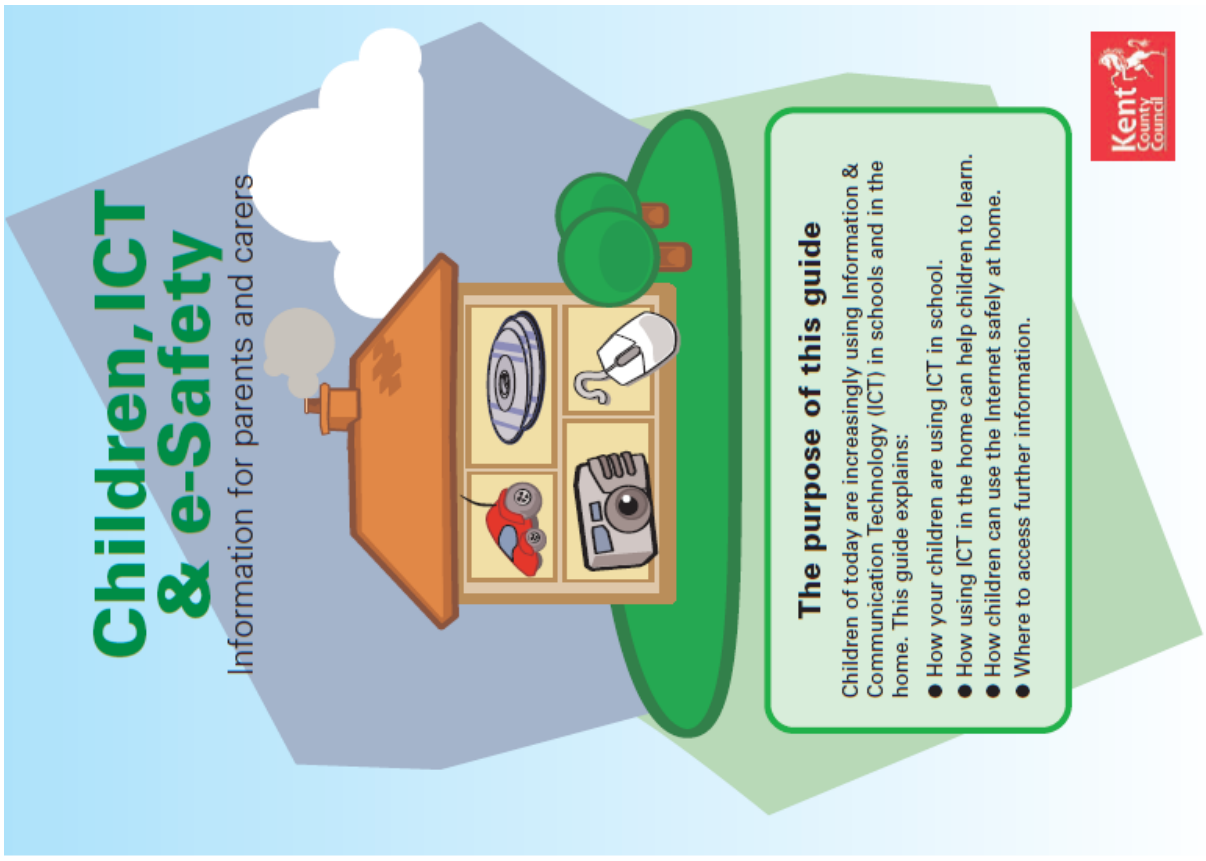
At Madginford Primary School we are happy for parents/carers to take photos and video of school events for personal use, but request that these images are not distributed or placed online. This is to protect all members of the school community.

Further Information on the Use of Images and video:

- Information Commissioner's Office: http://www.ico.org.uk
- Think U Know: http://www.thinkuknow.co.uk/
- Get Safe Online: www.getsafeonline.org
- Safety Net Kids: http://www.safetynetkids.org.uk

Appendix 10

Children, ICT & Online Safety – Information Leaflet



Using the Internet safely at home

Whilst many Internet Service Providers offer filtering systems to help you safeguard your child at home, it remains surprisingly easy for children to access inappropriate material including unsuitable texts, pictures and movies. Parents are advised to set the security levels within Internet Explorer with this in mind. Locating the computer in a family area, not a bedroom, will enable you to supervise children as they use the Internet. However, don't deny your child the opportunity to learn from the wide variety of material and games available on the Internet. Instead set some simple rules for keeping them safe and make sure they understand their importance.

Simple rules for keeping your child safe

To keep your child safe they should:

- ask permission before using the Internet
- only use websites you have chosen together or a child friendly search engine
- only email people they know, (why not consider setting up an address book?)
- ask permission before opening an email sent by someone they don't know
- not use Internet chat rooms
- not use their real name when using games on the Internet, (create a nick name)
- never give out a home address, phone or mobile number
- never tell someone they don't know where they go to school
- never arrange to meet someone they have 'met' on the Internet
- only use a webcam with people they know
- tell you immediately if they see anything they are unhappy with.

Some useful websites

When searching the Internet we recommend you use one of the following child friendly search engines:

Ask Jeeves for kids: www.askforkids.com

Yahooligans: www.yahooligans.com

CBBC Search: www.bbc.co.uk/cbbc/search

Kidsclick: www.kidsclick.org

Zoo Search: www.zoo.com

Using these rules

Go through these rules with your child and pin them up near to the computer. It is also a good idea to regularly check the Internet sites your child is visiting e.g. by clicking on History and Favourites. Please reassure your child that you want to keep them safe rather than take Internet access away from them.

For further information go to:

CEOP: www.ceop.gov.uk

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet-int.org

Kent County Council | Children, Families & Education Directorate | ASK

Appendix 11

Online Safety Audit Form

The Online Safety Policy was agreed by Governors:	28 September 2026
The next review is due:	September 2027
The Online Safety Policy is available for staff:	Staffroom and shared drive
The Online Safety Policy is available for parents/carers:	Via School Website
Responsible Senior Leadership Team member:	Claire Allen / Lisa Stamp
Governor responsible for Online Safety:	Toby Butler
Designated Child Protection Coordinator:	Claire Allen / Lisa Stamp
School Online Safety Coordinator:	Claire Allen / Lisa Stamp

Checklist

Has up-to-date Online Safety training been provided for all staff?	Yes / No
Do all staff sign the ICT Acceptable Use Policy on appointment?	Yes / No
Are all staff made aware of school expectations for safe/professional online behaviour?	Yes / No
Is there a clear procedure for staff, pupils and parents/carers to follow when responding to or reporting an Online Safety concern?	Yes / No
Have Online Safety materials from CEOP, Childnet, etc been obtained?	Yes / No
Is Online Safety training provided for all pupils appropriate to age/ability?	Yes / No
Are Online Safety rules displayed in all rooms with computers in a form accessible to all pupils?	Yes / No
Do parents/carers or pupils sign an Acceptable Use Policy?	Yes / No
Are staff, pupils, parents/carers and visitors aware that their network and Internet use is closely monitored and can be tracked?	Yes / No
Has an ICT security audit been initiated by SLT?	Yes / No
Is personal data collected, stored and use in accordance with the principles of the Data Protection Act?	Yes / No
Is Internet access via an approved educational service provider complying with DfE requirements?	Yes / No
Has the school filtering been designed to reflect educational objectives and approved by SLT?	Yes / No
Are staff responsible for managing filtering, network access and monitoring systems adequately supervised by a SLT member?	Yes / No
Does the school log and record all Online Safety incidents and actions?	Yes / No
Are the Governing Board and SLT monitoring and evaluating the school Online Safety Policy and ethos regularly?	Yes / No