	North Wootton Academy **Priory Lane** **North Wootton** **Kings Lynn** **Norfolk** **PE30 3PT**
Name of policy:	**Online Safety Policy**
Lead member of staff with responsibility for this policy:	Mr J Grimsby
Date of governors meeting when policy agreed:	NA
Type of governors meeting:	Academy Council
Date of implementation:	September 2026
Details of dissemination:	This policy is available on our school website. The policy is available for all staff, visitors, pupils and parents.
Frequency for review:	Annually
Next due for review:	September 2028

1. Contents

1. Aims 3
2. Legislation and guidance 4
3. Roles and responsibilities 4
4. Educating pupils about online safety 7
5. Educating parents/carers about online safety 8
6. Cyber-bullying 8
7. Acceptable use of the internet in school 10
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 11
10. How the school will respond to issues of misuse 11
11. Training 11
12. Monitoring arrangements 12
13. Links with other policies 12

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 13
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) 14
Appendix 3: online safety training needs – self-audit for staff 15
Appendix 4: online safety incident report log 16

1. 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- **Promote children's digital wellbeing and "online health", recognising that online safety is closely connected to physical health, sleep, mental wellbeing, relationships, learning, physical activity and healthy development.**
- **Help pupils develop age-appropriate digital literacy, critical thinking and resilience so that they can recognise misinformation, manipulation, harmful content, unsafe contact and emerging online risks.**
- **Ensure that emerging technologies, including generative artificial intelligence (AI), are considered within the school's safeguarding, data protection, curriculum and acceptable-use arrangements.**
- **Support pupils and families to develop healthy and balanced technology habits, including appropriate boundaries around recreational screen use, sleep, physical activity and sedentary behaviour.**

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, **misinformation and disinformation, harmful or misleading AI-generated content,** 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 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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; **the misuse of AI to impersonate, manipulate, harass, threaten or humiliate others;** and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams, **including scams and persuasive commercial activity facilitated by AI or personalised algorithms.**

The school recognises that these categories can overlap and that a single incident may involve several types of risk.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education 2026 (KCSIE 2026)**, and relevant DfE advice and standards relating to:

- **Keeping Children Safe in Education 2026**
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying
- **Relationships, Sex and Health Education (RSHE), including the updated statutory guidance applying from September 2026**
- Searching, screening and confiscation
- **Meeting digital and technology standards in schools and colleges: filtering and monitoring**
- **Generative AI: product safety standards**
- **Safe use of generative AI in education**
- **Data protection in schools and relevant UK GDPR/Data Protection Act requirements**
- **The Online Safety Act 2023 and relevant Ofcom requirements**

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, the Education Act 2011, the Data Protection Act 2018 and **the Online Safety Act 2023, where relevant to the school's responsibilities and the services used by pupils and staff.**

The school will keep this policy under review to reflect changes in legislation, statutory guidance, regulatory requirements and emerging online harms.

The policy also takes into account the National Curriculum computing programmes of study **and the school's responsibilities to provide age-appropriate education about online safety, digital literacy, media literacy, artificial intelligence and healthy technology use.**

The Government's July 2026 response to the "Growing Up in the Online World" consultation has also informed this policy. The Government has announced plans for social-media services to be restricted for children under 16, alongside stronger age assurance and restrictions on harmful online functions. These measures are not treated as current law within this policy until the relevant legislation comes into force. The school will respond to any future statutory requirements when they are confirmed.

3. Roles and responsibilities

3.1 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 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 their safeguarding needs.
- **Considering the safeguarding implications of AI-generated content and AI-enabled services when reviewing filtering and monitoring arrangements.**
- **Ensuring that filtering and monitoring arrangements are appropriately tested, understood by relevant staff and supported by clear procedures for responding to alerts and incidents.**

The governor who oversees online safety is Oliver Whitby.

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 the whole-school 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).
- **Ensure that the school considers the particular online risks faced by pupils with SEND, disadvantaged pupils and other children who may be especially vulnerable to online harm.**
- **Ensure that the school considers digital wellbeing, including the impact of technology on sleep, physical activity, sedentary behaviour, relationships and emotional wellbeing.**

3.2 The Principal

- The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- **The Principal will ensure that online safety remains an integral part of the school's safeguarding arrangements and that emerging online harms, including AI-related risks, are considered within the school's annual safeguarding risk assessment.**
- **The Principal will ensure that any proposed use of new digital or AI tools is appropriately risk assessed and approved before being used with pupils.**
- **The Principal will ensure that the school does not routinely monitor pupils' personal social-media accounts. Where information about a pupil's online activity is brought to the school's attention or there is a safeguarding or behaviour concern, the school will respond proportionately and in accordance with safeguarding, behaviour and data protection requirements.**

3.3 The designated safeguarding lead

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

The DSL (who is also the Principal and Computing Lead) takes lead responsibility for online safety in school, in particular:

- Supporting staff to understand this policy and ensuring that it is implemented consistently throughout the school.
- Working with the 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 Principal, 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 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.

- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face online.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually.
- **Ensuring that staff understand how online harms can present as safeguarding concerns, including grooming, exploitation, sexual harassment, abuse, coercive behaviour, radicalisation, bullying, self-harm and exposure to harmful or illegal content.**
- **Ensuring that staff understand the safeguarding implications of pupils interacting with generative AI tools, including inappropriate content, emotional dependency, manipulation, harmful advice, privacy risks and the disclosure of personal information.**
- **Ensuring that AI-related safeguarding incidents are recorded, assessed and escalated in accordance with the school's safeguarding procedures.**
- **Ensuring that concerns arising from AI-generated images, audio or video, including deepfakes or manipulated images of pupils, are treated as potential safeguarding concerns and responded to appropriately.**

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT management is provided through the trust via Turniton, who are 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, including terrorist and extremist material.
- **Ensuring that filtering systems take account of AI-generated content and emerging online threats, where technically possible and appropriate.**
- 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 weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- **Ensuring that technical safeguards are appropriately configured for the age of pupils and the school's educational context.**
- **Supporting the school in maintaining appropriate security, access controls, account management and data protection arrangements for AI and other digital services.**

In addition, the school Operations Lead and Principal ensure that:

- Any online safety incidents are logged and dealt with appropriately.

- Any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- **Any failures or weaknesses in filtering and monitoring are reported promptly to the DSL and ICT provider and acted upon.**

3.5 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 (appendices 1 and 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 recording on CPOMS and alerting the safeguarding team.
- Following the correct procedures by speaking with the Principal 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 and dealt with appropriately.
- 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'.
- **Never using unapproved AI tools with pupil personal data or confidential school information.**
- **Checking that AI-generated information is accurate, age-appropriate and suitable before using it in teaching or sharing it with pupils.**
- **Being alert to the possibility that AI-generated material may be inaccurate, biased, misleading, manipulative or harmful.**
- **Reporting suspected AI-related safeguarding incidents through the school's safeguarding procedures.**
- **Supporting pupils to take breaks from prolonged screen-based activity and to balance digital learning with movement, social interaction and other activities.**

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Principal 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.
- **Take reasonable steps to support their child's online safety and healthy technology use at home.**

- **Discuss with their child the importance of age-appropriate online services, privacy, passwords, respectful behaviour and reporting concerns.**
- **Follow relevant minimum-age requirements and parental controls for online services and games.**
- **Recognise that the Government has announced plans to restrict social-media services for under-16s. Until any new legislation comes into force, families should follow the existing age requirements and the terms of individual services.**

Parents/carers can seek further guidance on keeping children safe online from organisations including:

- UK Safer Internet Centre
- Childnet
- Internet Matters
- NSPCC
- **Government online safety and digital wellbeing resources**

3.7 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.

---

4. Educating pupils about online safety

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

All schools have to teach:

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

Online safety education will be age-appropriate, progressive and adapted to the needs and developmental stage of pupils. It will address both the opportunities and risks associated with technology.

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.
- **Understand that not everything they see or hear online is true.**
- **Understand that they should tell a trusted adult if something online makes them feel worried, uncomfortable, confused or unsafe.**
- **Develop simple healthy-use habits, including taking breaks from screens and making time for sleep, play, physical activity and face-to-face relationships.**

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.
- **Understand how algorithms, recommendations, advertising and persuasive design can influence what they see and how long they remain online.**
- **Recognise misinformation, disinformation, manipulated images, deepfakes and other misleading digital content.**
- **Understand the basic nature and limitations of AI, including that AI systems can produce inaccurate or inappropriate information and do not have feelings, consciousness or human judgement.**
- **Understand that AI-generated images, audio and video can be used to impersonate people or create misleading representations of real events.**
- **Understand that they should never share personal, private or sensitive information with an AI system unless explicitly instructed to do so by a trusted adult using an approved school system.**
- **Understand that AI should not replace human relationships, trusted adults or professional help.**
- **Understand how online behaviour can affect physical and mental wellbeing, including sleep, concentration, physical activity and relationships.**
- **Develop strategies for managing screen use, notifications, gaming and other online activities so that technology does not displace sleep, physical activity, learning, family life or social interaction.**
- **Understand that online services may have minimum-age requirements and that children should not misrepresent their age to access services.**

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.
- **How to identify and respond to misinformation, disinformation and manipulated or AI-generated content.**
- **That AI systems can make mistakes, generate false information, reproduce bias and produce content that is unsuitable for children.**
- **That they should not rely on AI systems for advice about health, relationships, safety or personal problems and should seek help from a trusted adult.**
- **That deepfakes and other AI-generated or manipulated content can be used to deceive, bully, harass, exploit or harm people.**
- **That personal information, photographs, voice recordings and other identifying information can be copied, altered, shared or misused once placed online.**

- **How to report harmful content, inappropriate contact, bullying, grooming, exploitation and other online concerns.**
- **How healthy digital habits can support sleep, physical health, learning, relationships and emotional wellbeing.**

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

The school will provide age-appropriate education about the Government's developing approach to social media age restrictions. Pupils will be taught that online services have age requirements and that they should follow the rules applicable to their age. The school will update its teaching and communications when any new statutory social-media restrictions come into force.

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

The school will take account of the fact that pupils may have very different levels of access to technology and different experiences of online life outside school.

Online health and healthy screen use

The school recognises "online health" as part of pupils' wider health and wellbeing. Technology can support learning, creativity, communication and accessibility, but excessive or poorly managed recreational screen use can displace sleep, physical activity, face-to-face interaction and other aspects of healthy development.

The UK Chief Medical Officers' guidance states that children and young people aged 5 to 18 should undertake an average of at least 60 minutes of moderate-to-vigorous physical activity per day across the week and should minimise sedentary time, breaking up long periods of inactivity with physical activity where possible.

The school will therefore:

- **Avoid unnecessary prolonged periods of sedentary screen use.**
- **Build opportunities for movement and physical activity into the school day.**
- **Encourage pupils to take appropriate breaks during extended screen-based learning.**
- **Teach pupils that recreational screen use should be balanced with sleep, physical activity, outdoor play, social interaction, reading and other offline activities.**
- **Promote healthy digital routines rather than focusing solely on a fixed number of minutes of screen use.**
- **Share forthcoming DfE guidance for parents of children aged 5–16 on screen use when that guidance is published.**

The school recognises that screen use should be considered in context, including its purpose, content, timing, impact on sleep and activity, and the individual needs of the child.

---

5. 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 or parent awareness sessions. This policy will also be shared with parents/carers.

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.
- **What AI tools, where applicable, pupils may encounter through school and the safeguards applied to their use.**
- **The school's expectations around mobile phones, social media, gaming and other online services.**
- **How parents/carers can support healthy online habits, including appropriate routines around sleep, physical activity, sedentary behaviour and recreational screen use.**
- **That the Government is developing evidence-based screen-time guidance for parents of children aged 5–16 and that this guidance will be shared with families when published.**
- **That the Government has announced plans to prevent social-media services being offered to under-16s, subject to the necessary legislation and implementation arrangements.**

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

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

---

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Cyber-bullying may also involve AI-generated or manipulated content, fake accounts, impersonation, deepfakes, altered images, synthetic audio or other technologies used to embarrass, threaten, harass or humiliate another person.

6.2 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 uses a 'If in doubt, minimise and shout out' approach to anything of concern online.

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

This will include education about AI-assisted bullying, including the creation or manipulation of photographs, audio or video, impersonation and the use of AI to generate abusive or threatening messages.

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.

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.

The school also asks that parents and families share any concerning interactions online with the school if they are between our pupils to allow the school to deal with this as a behaviour issue as if it had happened in school.

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 relevant material to the police as soon as is reasonably practicable, where there are reasonable grounds to suspect that possessing or distributing the material is illegal, **and will seek advice where there is uncertainty about the legal or safeguarding position.**

They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Pupils in Year 5/6 are able to bring a phone into school so long as parents/families give permission through an electronic form and, in doing so, acknowledge our expectations of use.

The use of these devices is primarily for school travel and therefore they are passed to the class teacher and secured for the school day.

However, should there be an incident, the Principal, or a member of the Senior Leadership Team in their absence, can carry out a search and confiscate any electronic device where there are reasonable grounds for suspecting that it:

- 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.

Any search will be carried out in accordance with the DfE's current Searching, Screening and Confiscation guidance and the school's behaviour policy.

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 Principal.
- 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.

The Senior Leadership Team may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where this is permitted under current DfE guidance and where they have 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 Principal 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.

Where material may constitute evidence of an offence, staff must preserve the evidence and seek appropriate advice rather than deleting it.

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 unnecessarily.
- Not copy, save, forward or distribute the image.

- Confiscate the device where appropriate and report the incident to the DSL immediately.
- **Follow the DfE's current guidance on responding to nude and semi-nude images and the school's child protection procedures.**

The school will take particular care where AI has been used to create or manipulate an image of a child. A sexually explicit AI-generated or manipulated image involving a child may raise serious safeguarding and legal concerns even where the image does not depict an actual event. Staff must not circulate such material.

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

- The DfE's latest guidance on searching, screening and confiscation.
- **The DfE's current safeguarding guidance on responding to nude and semi-nude images.**
- Our behaviour policy.
- Our child protection and safeguarding 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.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) is developing rapidly and is increasingly embedded within search engines, apps, games, social-media platforms, educational technology and other online services. The school recognises both its educational potential and the safeguarding, developmental, privacy and wellbeing risks it can present to primary-aged children.

The school will only permit pupils to use AI tools where the tool has been appropriately assessed and approved by the school. Pupils will not be expected to create personal accounts on general-purpose AI services for school work unless specifically authorised and appropriate safeguards are in place.

The school recognises the following particular risks for primary-aged pupils:

- **Exposure to inappropriate, sexual, violent, hateful or otherwise harmful content generated in response to apparently innocent questions.**
- **AI hallucinations or fabricated information being presented as fact.**
- **Children developing an inappropriate level of trust in AI systems or treating them as if they were human friends, confidants or trusted adults.**
- **Emotional dependency or excessive engagement with conversational AI.**
- **AI systems providing inappropriate advice about health, relationships, emotions or personal problems.**
- **Children disclosing personal, family, school, location or other sensitive information to AI systems.**
- **AI-generated images, audio and video being used to deceive, impersonate, bully or humiliate people.**
- **Deepfakes and manipulated images being used to create false representations of children or adults.**

- **AI being used to facilitate grooming, coercion, exploitation, fraud, scams or other harmful behaviour.**
- **Exposure to persuasive, manipulative or commercially motivated AI interactions.**
- **AI reducing opportunities for children to develop their own reasoning, creativity, writing, problem-solving and decision-making skills if it completes tasks for them.**
- **Bias and stereotypes being reproduced or amplified by AI systems.**
- **Children encountering AI systems through platforms or services whose minimum age is above the child's age.**
- **AI-generated misinformation and disinformation making it harder for children to distinguish reliable information from fabricated or manipulated content.**

When teaching about AI, the school will emphasise that AI is a tool and not a person. Pupils will be taught that AI does not replace trusted adults, teachers, parents/carers, friendships or professional support.

Where AI is used for educational purposes, staff will:

- **Use only school-approved tools.**
- **Check the age suitability, safeguarding arrangements and privacy/data-processing arrangements of the tool.**
- **Not enter personal, confidential or sensitive information into AI tools unless this has been specifically authorised and appropriate data protection arrangements are in place.**
- **Check AI-generated content for accuracy, bias, appropriateness and safeguarding risks before using it.**
- **Ensure AI use supports rather than replaces pupils' thinking and learning.**
- **Follow the DfE's generative AI product safety standards and relevant data protection requirements.**

Where learner-facing AI tools are considered for use, the school will consider whether the product provides appropriate safeguards around harmful content, monitoring, data protection, cognitive development, emotional and social development, mental health and manipulation.

The school will treat any use of AI to bully, harass, impersonate, threaten or otherwise harm pupils in line with the behaviour, anti-bullying and safeguarding policies.

Any AI-generated material that suggests a safeguarding concern will be reported to the DSL. Staff should not investigate potentially harmful material independently where doing so could increase the risk to the child or compromise evidence.

The school will provide age-appropriate education about deepfakes, misinformation and AI-generated content. Primary pupils will be taught that images, audio and video can be manipulated and that seeing something online does not necessarily mean that it is genuine.

The school will monitor developments in Government policy concerning AI. The Government has announced further measures concerning AI chatbots, including restrictions on sexualised AI chatbot services for under-18s and additional

safeguards for children. These measures will be incorporated into school procedures as relevant when they come into force.

The school will also recognise the importance of healthy AI use. Where learner-facing AI tools are used, staff will ensure that use is purposeful and time-limited, that pupils have opportunities to work away from screens, and that AI use does not displace physical activity, social interaction, play, sleep or other healthy activities.

7. 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.

Filtering and monitoring will be proportionate, age-appropriate and designed to protect users without unreasonably restricting legitimate teaching and learning.

AI-generated content and AI-enabled services will be included within the school's consideration of filtering and monitoring risks.

More information is set out in the Trust's acceptable use agreements.

8. Pupils using mobile devices in school

The school operates a phone-free environment in accordance with current DfE expectations and school rules.

Pupils in Year 5/6 may bring mobile devices into school, but these must be handed to the class teacher and not be visible or accessible on the school site during the school day.

Pupils must not use mobile phones, smart watches or other personal smart devices to access social media, messaging services, gaming, cameras or other online services during the school day unless specifically authorised by a member of staff for an educational or safeguarding purpose.

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.

The school will keep its mobile-device arrangements under review in light of changes to DfE guidance and Government policy.

The school will also recognise the relationship between mobile-phone use, notifications, sleep, concentration, physical activity and wellbeing when educating pupils and parents/carers about healthy technology use.

---

9. 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.
- **Using strong, unique passwords and multi-factor authentication where provided.**
- No external hard drives should be used unless authorised; documents should be saved securely using the school's approved storage systems.
- 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 where required.
- Keeping operating systems up to date by always installing the latest updates.
- **Using only school-approved software, cloud services and AI tools for school business.**
- **Not entering pupil, parent/carer, staff or other confidential information into unapproved AI systems.**
- **Taking particular care when using AI systems remotely to ensure that personal and confidential information is not disclosed.**

Staff members must not use the device in any way that would violate the school's terms of acceptable use which they sign at the start of their time at the school.

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 Principal **and/or ICT support immediately.**

---

10. 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 misuse involves AI, the school will consider both the nature of the AI-generated or AI-assisted material and the way in which it was used.

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.

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

Safeguarding concerns will be referred to the DSL without delay. The school will not assume that an incident is merely a behaviour issue where there may be a safeguarding element.

Where an online incident occurs outside school but involves pupils or has a significant impact on pupils' safety or wellbeing, the school will consider whether it has safeguarding or behaviour responsibilities and will respond accordingly.

Where an incident involves a third-party platform, the school may also consider whether the matter should be reported to the platform, the relevant service provider, the local authority, the police or another appropriate agency.

---

11. 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.

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.
  - Sharing of abusive images and pornography with those who do not want to receive such content.
  - **AI-generated or manipulated images, audio or video.**
  - **Impersonation, fake accounts and AI-generated abusive content.**
- Physical abuse, sexual violence and initiation/hazing-type violence can all contain an online element.
- **AI can create additional safeguarding risks, including harmful content, manipulation, emotional dependency, misinformation, privacy risks and the generation or alteration of images and other media.**
- **Online harms can affect pupils' physical health, mental wellbeing, sleep, relationships, concentration and ability to learn.**

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 healthy long-term choices and keep them safe from harm in the short term.
- **Understand the safeguarding and data-protection implications of AI use.**
- **Understand how to respond appropriately when pupils disclose concerns arising from AI, social media, gaming or other digital services.**
- **Understand the school's filtering and monitoring arrangements and how to report failures or safeguarding alerts.**
- **Understand the importance of healthy digital habits, including movement, breaks from prolonged sedentary behaviour, sleep and balanced recreational screen use.**

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.

Staff training will be updated when significant new online risks emerge, including developments in AI, online exploitation, social-media regulation and other emerging technologies.

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

---

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

The school will monitor filtering and monitoring alerts and incidents in accordance with its technical arrangements and safeguarding procedures. Monitoring will be used to identify potential safeguarding concerns, inappropriate use and weaknesses in filtering.

The school will review online safety incidents for patterns or emerging risks, including repeated concerns involving particular platforms, technologies, online communities or forms of AI-generated content.

This policy will be reviewed every year by the Principal who is the online safety lead.

At every review, the policy will be shared with the governing board.

The review 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 annual review will consider, where relevant:

- **Emerging online harms and safeguarding trends.**
- **Developments in AI and generative AI.**
- **The effectiveness of filtering and monitoring.**
- **Mobile-phone and personal-device use.**
- **Pupil and parent/carer feedback.**
- **Incidents involving social media, gaming, messaging and online communities.**
- **Digital wellbeing, including screen use, sedentary behaviour, sleep and physical activity.**
- **Changes to DfE guidance, KCSIE, the Online Safety Act, Ofcom requirements and Government policy.**
- **Any new statutory requirements arising from the Government's "Growing Up in the Online World" programme.**

The school will update this policy between annual reviews where significant changes in law, statutory guidance or safeguarding risks require an earlier amendment.

---

13. 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
- Internet acceptable use policy
- **Mobile phone policy / arrangements**
- **RSHE and Health Education policy**
- **Computing curriculum policy**
- **Mental health and wellbeing policy, where applicable**
- **Attendance policy, where relevant to online learning**
- **Educational visits and remote learning arrangements, where relevant**

Key changes I would recommend before adoption

There are a few points in your original policy that I would **not** simply leave as they were:

229. **Remove the "annual social media search" of pupils.**
I have replaced this with proportionate safeguarding monitoring. A routine trawl of pupils' personal social-media accounts creates significant privacy, proportionality and data-protection questions and isn't a standard KCSIE requirement.
230. **Correct the AI section substantially.**
The DfE's current AI safety standards now go much further than simply warning about deepfakes. They specifically address **harmful content, data protection,**

cognitive offloading, emotional dependency, mental health, manipulation, monitoring and child safety. G GOV.UK

231. **Don't write that the under-16 social-media ban is already law.**
The Government has announced the policy following the 2026 consultation, but the Government's own children's summary states that **Parliament must approve the new laws before the plans come into effect**. G GOV.UK

232. **I would use "online health" as a school wellbeing concept rather than promising a fixed screen-time allowance.**
The current Chief Medical Officers' guidance says 5–18-year-olds should average at least **60 minutes of moderate-to-vigorous physical activity per day across the week**, minimise sedentary time and break up prolonged periods of inactivity.

G GOV.UK The Government has also said its forthcoming 5–16 screen-time guidance will consider **duration, content, context and the individual child**, rather than simply imposing a universal number of minutes.

G GOV.UK

233. **The mobile-phone section should be checked against your Trust's actual policy.**
The Government has strengthened its expectation that schools should be phone-free, including during lessons, breaks and lunchtime, so your existing Year 5/6

arrangement should be explicitly consistent with the Trust's current mobile-phone policy. GOV.UK

234. **The KCSIE reference should now say 2026.**
KCSIE 2026 came into force on **1 September 2026**, replacing the 2025 version.
GOV.UK

For formal adoption, I would also recommend that the **appendices are rewritten**, particularly the EYFS/KS1 and KS2 acceptable-use agreements, so that the child-facing wording reflects the new AI, social-media, mobile-phone and online-health provisions rather than leaving the main policy updated but the agreements out of date.

Sources

2. You said:

Can you make this shorter maybe around 40% shorter

3. ChatGPT said:

Absolutely. I'd keep the same structure but remove repetition, combine overlapping responsibilities, and make the AI/online-health sections concise while retaining the important **KCSIE 2026, DfE, AI, social-media and safeguarding requirements**.

I can produce a **roughly 40% shorter version with all substantive changes still in bold**, rather than simply cutting paragraphs at random.

4. You said:

Yes please

5. ChatGPT said:

Below is a more concise version, retaining your original structure and **bolding substantive changes/additions**. I've aimed to remove repetition while keeping the policy suitable for formal school adoption.

Online Safety Policy

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Monitoring arrangements
13. Links with other policies

Appendix 1: EYFS and KS1 acceptable use agreement
Appendix 2: KS2, KS3 and KS4 acceptable use agreement
Appendix 3: Online safety training needs – self-audit for staff
Appendix 4: Online safety incident report log

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support pupils who may be at greater risk of harm online.
- Deliver an effective approach to online safety which protects and educates the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate online safety concerns.
- **Promote children's "online health", recognising the links between technology use, physical activity, sedentary behaviour, sleep, mental wellbeing, relationships and learning.**
- **Develop pupils' digital literacy, critical thinking and resilience, including their ability to recognise misinformation, manipulation and AI-generated content.**

The 4 key categories of risk

Our approach is based on four categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, including pornography, misinformation, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism and harmful AI-generated content.
- **Contact** – harmful interaction with other users, including peer pressure, advertising, grooming, exploitation and adults pretending to be children.
- **Conduct** – online behaviour that causes or increases the likelihood of harm, including bullying, sharing explicit images, harassment, impersonation and the misuse of AI.
- **Commerce** – risks including gambling, inappropriate advertising, phishing, scams and other financial exploitation.

---

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education 2026 (KCSIE 2026)**, and relevant DfE guidance on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying.
- **Relationships, Sex and Health Education (RSHE).**
- Searching, screening and confiscation.
- **Filtering and monitoring standards.**
- **Generative AI and product safety.**
- Data protection and privacy.
- Protecting children from radicalisation.

It reflects relevant legislation, including the Education Acts, Equality Act 2010, Data Protection Act 2018 and **Online Safety Act 2023 and relevant Ofcom requirements**.

It also takes account of the National Curriculum computing programmes of study.

The policy will be reviewed in response to changes in legislation, statutory guidance and emerging online risks.

The Government's response to the 2026 "Growing Up in the Online World" consultation has informed this policy. The Government has announced plans to restrict social-media services for under-16s, subject to legislation. The school will not treat these proposals as current law until the relevant legislation comes into force.

---

3. Roles and responsibilities

3.1 The governing board

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

The governing board will:

- Ensure staff receive appropriate online safety and safeguarding training.

- Ensure online safety is embedded throughout the school's safeguarding arrangements.
- Ensure appropriate filtering and monitoring systems are in place and reviewed at least annually.
- Ensure staff understand their responsibilities for filtering and monitoring and know how to report concerns.
- Ensure online safety education is adapted for vulnerable pupils and pupils with SEND.
- **Ensure online health, including the relationship between technology use, physical activity, sedentary behaviour and wellbeing, is considered within the school's approach.**
- **Ensure emerging risks, including AI, are considered within safeguarding risk assessments.**

The governor who oversees online safety is Oliver Whitby.

All governors will read and understand this policy and adhere to the school's acceptable-use requirements.

3.2 The Principal

The Principal is responsible for ensuring that staff understand and implement this policy consistently.

The Principal will:

- **Ensure online safety remains an integral part of safeguarding and annual risk assessment processes.**
- **Ensure new digital and AI tools are appropriately assessed and approved before use with pupils.**
- **Ensure the school does not routinely monitor pupils' personal social-media accounts. Where concerns are raised, they will be addressed proportionately and in accordance with safeguarding, behaviour and data protection requirements.**

3.3 The designated safeguarding lead

The DSL takes lead responsibility for online safety and will:

- Support staff to implement this policy.
- Work with the governing board to review the policy annually.
- Understand and oversee filtering and monitoring arrangements.
- Manage online safety incidents in accordance with the child protection policy.
- Ensure incidents are appropriately recorded and escalated.
- Provide regular online safety and safeguarding updates to staff.
- Liaise with external agencies where necessary.
- Undertake annual risk assessments relating to online harm.
- **Ensure staff understand emerging risks, including grooming, exploitation, sexual harassment, cyber-bullying, radicalisation and AI-related harm.**
- **Ensure AI-related safeguarding incidents, including deepfakes and manipulated images, are dealt with through safeguarding procedures.**

This list is not exhaustive.

3.4 The ICT manager

The ICT management is provided through the Trust via Turniton, who are responsible for:

- Maintaining appropriate filtering and monitoring systems and reviewing their effectiveness at least annually.
- Protecting ICT systems against malware and other security threats.
- Conducting regular security checks and monitoring.
- Blocking access to harmful or inappropriate sites and files where possible.
- **Supporting appropriate security and data-protection arrangements for approved AI and digital services.**
- **Reporting failures in filtering or monitoring promptly to the DSL and school leadership.**

The Operations Lead and Principal will ensure incidents are logged and dealt with appropriately.

3.5 All staff and volunteers

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

- Understanding and implementing this policy.
- Following acceptable-use requirements.
- Reporting filtering or monitoring failures through CPOMS and to the safeguarding team.
- Seeking permission before bypassing filtering systems for educational purposes.
- Reporting and responding appropriately to online safety and cyber-bullying incidents.
- Responding appropriately to concerns about sexual violence and harassment, maintaining an attitude of "it could happen here".
- **Using only approved AI tools and never entering personal, confidential or sensitive information into unapproved AI systems.**
- **Checking AI-generated content for accuracy, appropriateness and safeguarding risks.**
- **Supporting pupils to take appropriate breaks from prolonged screen use.**

3.6 Parents/carers

Parents/carers are expected to:

- Raise online safety concerns with the school.
- Ensure their child understands the school's acceptable-use requirements.
- **Support age-appropriate and healthy technology use at home, including appropriate boundaries around sleep, physical activity and recreational screen use.**
- **Follow age requirements for online services and discuss online safety, privacy and reporting concerns with their children.**

Parents/carers can seek further guidance from organisations including UK Safer Internet Centre, Childnet, Internet Matters and the NSPCC.

Parents will be informed of relevant changes to Government policy concerning social-media age restrictions and screen-time guidance.

3.7 Visitors and members of the community

Visitors using the school's ICT systems will be made aware of this policy and, where appropriate, agree to the acceptable-use requirements.

---

4. Educating pupils about online safety

Pupils will be taught online safety as part of the curriculum, including through computing, RSHE, PSHE and other relevant subjects.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully and keep personal information private.
- Identify where to seek help with online content or contact.
- **Understand that not everything online is true and tell a trusted adult if something online makes them feel worried or unsafe.**
- **Develop healthy technology habits, including taking breaks from screens.**

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify ways to report concerns.
- **Understand how algorithms, advertising and recommendations can influence what they see online.**
- **Recognise misinformation, manipulated images, deepfakes and AI-generated content.**
- **Understand that AI can make mistakes, produce inappropriate material and should not be treated as a human or trusted adult.**
- **Understand the importance of protecting personal information when using AI and other online services.**
- **Understand the impact of technology use on sleep, physical activity, relationships, concentration and wellbeing.**
- **Understand that online services have age requirements and that children should not misrepresent their age to access them.**

By the end of primary school, pupils will know:

- That people may behave differently online or pretend to be someone else.
- That the same principles of respect apply online and offline.
- How to recognise and report harmful content and contact.
- How to critically assess online friendships and sources of information.
- How information and data is shared and used.

- Appropriate boundaries in online relationships.
- How to respond safely to adults they do not know.
- **How AI-generated and manipulated content can be used to deceive, bully or harm people.**
- **That AI can generate false or biased information and should not replace trusted adults or professional advice.**
- **How to develop healthy digital habits and balance screen use with sleep, physical activity, social interaction, play and learning.**

The school will provide age-appropriate information about the Government's developing approach to social-media age restrictions. Existing age requirements will be followed until any new legislation comes into force.

Teaching will be adapted for vulnerable pupils, victims of abuse and pupils with SEND.

Online health

The school recognises online health as part of pupils' wider health and wellbeing. Technology can support learning and communication, but excessive recreational screen use can displace sleep, physical activity, social interaction and other healthy activities.

The school will:

- **Avoid unnecessary prolonged periods of sedentary screen use.**
- **Provide opportunities for movement and physical activity during the school day.**
- **Encourage breaks during extended screen-based learning.**
- **Teach pupils to balance recreational screen use with sleep, physical activity, outdoor play, relationships, reading and other offline activities.**
- **Share relevant Government guidance on screen use when the forthcoming 5–16 guidance is published.**

The school recognises current Chief Medical Officers' advice that children aged 5–18 should undertake an average of at least 60 minutes of moderate-to-vigorous physical activity each day across the week and minimise prolonged sedentary behaviour.

---

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness through communications, the website and parent sessions.

Parents/carers will be informed about:

- The school's filtering and monitoring systems.
- What children are asked to do online.
- **Any AI tools approved for pupil use and the safeguards applied.**
- **Mobile-phone and online-service expectations.**
- **Healthy screen use, including sleep, physical activity and sedentary behaviour.**
- **Relevant changes to Government policy on social media and screen use.**

Concerns should be raised with the Principal and/or DSL.

---

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online through platforms such as social networking sites, messaging apps and gaming services. It involves intentional harm where there is an imbalance of power.

It may also involve fake accounts, impersonation, AI-generated or manipulated images, audio or video, or AI-generated abusive messages.

6.2 Preventing and addressing cyber-bullying

The school will ensure pupils understand cyber-bullying, know how to report it and understand the impact on others.

The school uses a **"If in doubt, minimise and shout out"** approach to concerns online.

Cyber-bullying will be addressed through the behaviour and safeguarding procedures as appropriate. Parents/carers are encouraged to report concerning online interactions involving pupils.

Where illegal or harmful material has been shared, the school will take reasonable steps to contain the incident and involve the police or other agencies where appropriate.

AI-assisted bullying, including manipulated images or deepfakes, will be treated as a safeguarding and/or behaviour concern as appropriate.

6.3 Examining electronic devices

Pupils in Years 5 and 6 may bring a phone into school with parental permission. Devices must be handed to the class teacher and secured for the school day.

Where there are reasonable grounds to suspect that an electronic device:

- poses a risk to staff or pupils;
- is a prohibited item under the school's rules; or
- contains evidence relating to an offence,

an authorised member of staff may search and confiscate the device in accordance with the **DfE's current Searching, Screening and Confiscation guidance** and the school's behaviour policy.

Staff will explain the reason for the search and seek the pupil's cooperation wherever possible.

Where a device may contain illegal or harmful material, staff must not unnecessarily view, copy or distribute it and should seek advice from the DSL.

If a staff member suspects a device may contain a nude or semi-nude image of a child, they will:

- Not view or copy the image unnecessarily.
- Report the concern to the DSL immediately.
- Follow the school's safeguarding procedures and current DfE guidance.

Where AI has been used to create or manipulate a sexualised image involving a child, the material will be treated as a serious safeguarding concern and will not be circulated.

Any searching will comply with current DfE guidance, safeguarding procedures and the behaviour policy.

6.4 Artificial intelligence (AI)

Generative AI is developing rapidly and may be encountered through search engines, apps, games, educational platforms and other online services. The school recognises both its educational potential and the risks it presents to primary-aged pupils.

Key risks include:

- **Exposure to inappropriate or harmful content.**
- **False, inaccurate or biased information ("hallucinations").**
- **Children developing inappropriate trust or emotional dependency on AI systems.**
- **AI providing inappropriate advice about health, relationships or personal problems.**
- **Disclosure of personal or sensitive information.**
- **Deepfakes and manipulated images, audio or video.**
- **Impersonation, bullying, grooming, exploitation and scams.**
- **AI reducing opportunities for pupils to develop independent thinking, creativity and problem-solving.**
- **Exposure to services with age restrictions above the child's age.**

Pupils will be taught that AI is a tool, not a person, and does not replace parents, teachers, trusted adults or professional advice.

Where AI is approved for educational use, staff will:

- **Use only approved services.**
- **Consider age suitability, safeguarding, privacy and data protection.**
- **Not enter personal or confidential information into unapproved AI systems.**
- **Check AI-generated information and resources before using them.**
- **Ensure AI supports rather than replaces pupils' learning and thinking.**
- **Follow relevant DfE AI safety standards.**

Any AI-related safeguarding concern will be reported to the DSL.

The school will keep its AI arrangements under review as Government guidance and technology develop.

---

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to agree to the school's acceptable-use requirements.

Use of the school's internet must be for educational purposes or the fulfilment of an individual's role.

We will monitor internet use where appropriate and restrict access through filtering systems.

Filtering and monitoring will be proportionate, age-appropriate and designed to protect users without unnecessarily restricting teaching and learning.

AI-enabled services will be considered within the school's filtering, monitoring and safeguarding arrangements.

---

8. Pupils using mobile devices in school

Pupils in Years 5 and 6 may bring mobile devices into school, but these must be handed to the class teacher and must not be visible or accessible during the school day.

Mobile phones, smart watches and other personal smart devices must not be used to access social media, messaging, gaming or other online services during the school day unless specifically authorised.

Breaches may result in disciplinary action in accordance with the behaviour policy.

The school's arrangements will be reviewed in light of changes to DfE guidance and Government policy.

---

9. Staff using work devices outside school

Staff must take appropriate steps to keep work devices secure, including:

- Using strong passwords and multi-factor authentication where available.
- Saving documents using approved school storage systems.
- Ensuring devices lock when unattended.
- Not sharing devices with family or friends.
- Keeping security software and operating systems up to date.
- **Using only school-approved software, cloud services and AI tools.**
- **Never entering confidential pupil, parent/carer or staff information into unapproved AI systems.**

Work devices must be used in accordance with the school's acceptable-use requirements.

Security concerns must be reported to the Principal and/or ICT support.

---

10. How the school will respond to issues of misuse

Where a pupil misuses ICT systems or the internet, the school will follow the behaviour, safeguarding and acceptable-use procedures. Action will be proportionate to the circumstances.

Where AI is involved, the school will consider both the content and how it was created or used.

Staff misuse will be dealt with through the relevant disciplinary procedures.

The school will consider whether serious or illegal incidents should be reported to the police or another appropriate agency.

Safeguarding concerns will be referred to the DSL without delay and will not be treated solely as behaviour concerns where there may be a safeguarding element.

Online incidents occurring outside school may be addressed where they affect pupil safety, wellbeing or the school community.

---

11. Training

All new staff will receive online safety and safeguarding training as part of induction.

All staff will receive refresher training at least annually and relevant updates throughout the year.

Training will ensure staff understand:

- The role of technology in safeguarding and wellbeing.
- Online abuse, grooming, exploitation and cyber-bullying.
- Non-consensual sharing of nude and semi-nude images.
- Sexual harassment and violence with an online element.
- **AI-related risks, including harmful content, misinformation, deepfakes, manipulation, emotional dependency and privacy risks.**
- **The school's filtering and monitoring arrangements.**
- **The relationship between technology use, sleep, physical activity, sedentary behaviour and wellbeing.**

Training will support staff to identify signs of online harm and help pupils make healthy and safe choices.

The DSL and deputies will undertake safeguarding training at least every 2 years and update their online safety knowledge at least annually.

Governors and volunteers will receive appropriate training.

12. Monitoring arrangements

The DSL will log behaviour and safeguarding incidents relating to online safety.

The school will monitor filtering and monitoring alerts and review online safety incidents for patterns or emerging risks, including those involving AI, social media, gaming and messaging services.

This policy will be reviewed annually by the Principal and shared with the governing board.

The review will be supported by an annual risk assessment considering the risks pupils face online.

The review will consider:

- **Emerging online harms and AI developments.**
- **Filtering and monitoring effectiveness.**
- **Mobile-phone and personal-device use.**
- **Social-media and gaming-related concerns.**
- **Digital wellbeing, including screen use, sedentary behaviour, sleep and physical activity.**
- **Changes to KCSIE, DfE guidance, the Online Safety Act, Ofcom requirements and Government policy.**

The policy will be updated sooner where significant changes in law, guidance or safeguarding risks require this.

13. 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
- Internet acceptable use policy
- **Mobile phone policy**
- **RSHE and Health Education policy**
- **Computing policy**
- **Mental health and wellbeing policy, where applicable**

You'll get smarter responses and can upload files, images, and more.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR 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, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR 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 that 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 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: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways 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 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**