

St Wilfrid's CE Primary Academy

Hurst Education Trust

Online Safety Policy

Policy name	Online Safety Policy
Policy source	Adapted from The Key model policy (September 2026), with enhancements
Approved by	Full Governing Body Date: 10/7/2026
Last reviewed	July 2026
Review period	Annually
Next review due	July 2027
Signed (Headteacher)	Simon Hateley
Signed (Chair of Governors)	
Statutory linked guidance	Keeping Children Safe in Education; DfE Filtering and Monitoring Standards; Teaching Online Safety in Schools; Searching, Screening and Confiscation; Online Safety Act 2023

Contents

1. Aims	3
2. Legislation and guidance	4
3. Roles and responsibilities	5
4. Educating pupils about online safety	9
5. Educating parents and carers about online safety	11
6. Cyber-bullying and online harm	12
7. Acceptable use of the internet in school	16
8. Pupils using mobile devices in school	17
9. Staff using work devices outside school	17
10. How the school will respond to issues of misuse	18
11. Training	18
12. Monitoring arrangements	19
13. Links with other policies	19
Appendix 1. EYFS and KS1 acceptable use agreement	20
Appendix 2. KS2 acceptable use agreement	21
Appendix 3. Acceptable use agreement (staff, governors, PTA, visitors)	22
Appendix 4. Staff self-audit	23

1. Aims

St Wilfrid's CE Primary Academy 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 throughout as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Hold ourselves accountable to the standards set by Keeping Children Safe in Education and the Online Safety Act 2023.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk, as set out in Keeping Children Safe in Education:

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

These risks are not mutually exclusive; an incident may involve more than one category, and online and offline harm frequently overlap. Our approach reflects this throughout.

2. Legislation and guidance

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

- Teaching online safety in schools
- Meeting digital and technology standards in schools and colleges (including cyber security standards and filtering and monitoring standards)
- Preventing and tackling bullying, and cyber-bullying: advice for headteachers and school staff
- Relationships education, relationships and sex education (RSE) and health education (introduced 1 September 2026)
- Searching, screening and confiscation
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes
- Generative artificial intelligence in education

It also refers to the DfE's guidance on protecting children from radicalisation (Prevent duty).

It reflects existing legislation, including but not limited to:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011 (giving 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)
- Voyeurism (Offences) Act 2019
- Data Protection Act 2018 and UK GDPR
- Online Safety Act 2023 and associated Ofcom Codes of Practice, including child safety duties

The policy takes into account the National Curriculum computing programmes of study and complies with the school's funding agreement and articles of association as an academy within Hurst Education Trust.

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 delegate management of this to the headteacher and receive regular reports to:

- Ensure all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually.
- Co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- Ensure that the school teaches pupils how to keep themselves and others safe, including online.

The governor who oversees online safety is Sarah Milton-Hunt.

All governors will:

- Make sure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3).

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school. The headteacher supports the DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

The headteacher will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The headteacher will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and procedures.
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). 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.

3.3 The designated safeguarding lead (DSL)

Details of the school's DSL and deputy DSLs are set out in the school's Child Protection and Safeguarding Policy, as well as in relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and make sure procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT service provider to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT service provider 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 and Safeguarding Policy.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safety incidents with a safeguarding dimension are logged on CPOMS and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are logged on CPOMS 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, including the police, children's social care and the West Sussex Safeguarding Children Partnership.
- Providing termly reports on online safety in school to the headteacher and governing board.
- Undertaking annual risk assessments that consider and reflect the risks pupils face online.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually.

This list is not intended to be exhaustive.

3.4 The ICT service provider

St Wilfrid's CE Primary Academy engages an external ICT service provider (Entrust) to manage key aspects of the school's digital infrastructure, including filtering, monitoring, network security and device management. The School Business Manager and Headteacher are responsible for conducting appropriate due diligence on this provider, ensuring all necessary checks are completed prior to engagement, and carrying out regular reviews to confirm that services are delivered effectively, securely, and in alignment with the school's safeguarding and online safety standards.

The ICT service 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 termly to assess effectiveness and to ensure that pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure that the school's ICT systems are secure, with Two Factor Authentication being in place where the option is available, and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring of 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.
- Working with the DSL and headteacher to investigate alerts generated by filtering and monitoring systems (the school uses Securus for active monitoring; alerts are reviewed and logged in line with section 12 of this policy).
- Making sure that any technical incidents are escalated appropriately and that any safeguarding-related incidents are reported to the DSL without delay.

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 making sure 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 reporting to the DSL or headteacher and recording on CPOMS where the failure has a safeguarding dimension.

- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes — by submitting a written request to the Headteacher or Deputy Headteacher in advance.
- Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.
- 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'.
- Modelling good online behaviours and maintaining a professional level of conduct in their personal use of technology.

This list is not intended to be exhaustive.

3.6 Parents and carers

Parents and carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2).
- Support the school's approach to online safety, including by reinforcing key messages at home and modelling safe and respectful behaviour online themselves.

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

- What are the issues? — UK Safer Internet Centre
- Help and advice for parents and carers — Childnet
- Parents and carers resource sheet — Childnet
- ParentZone — practical guides for parents on apps, games and online trends
- Internet Matters — age-by-age advice
- National College

3.7 Pupils

Pupils are responsible for:

- Adhering to the acceptable use agreement (Appendix 1 or 2 as appropriate) and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3.8 Visitors, contractors, the PTA and members of the community

Visitors, contractors, members of the Parents and Teachers Association (PTA), and members of the community who use the school's ICT systems, the school's Wi-Fi, or the guest Wi-Fi network

will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3). Arrangements for non-staff users of the school's Wi-Fi, including the 24-hour guest code arrangement, are set out in section 7.2.

4. Educating pupils about online safety

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

Online safety is taught through our PSHE and computing curriculum and is reinforced across other subjects where relevant. The content below reflects the National Curriculum computing programmes of study and the government's renewed guidance on relationships education and health education (introduced 1 September 2026).

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.
- Recognise acceptable and unacceptable behaviour

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.
- Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.

- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

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.

4.2 Pupils will be taught practical cyber security skills

In line with the DfE's cyber security standards for schools and colleges, pupils will receive age-appropriate training on safe internet use, including:

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

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

4.3 Adapting teaching for vulnerable pupils

The DSL works with the SENCO and class teachers to ensure that online safety teaching is appropriately adapted for pupils who may be more vulnerable to online harm. This includes, but is not limited to:

- Pupils with SEND, where the risks and indicators of grooming, exploitation and online bullying may present differently.
- Pupils who are victims of, or have witnessed, abuse, for whom certain content or discussions may be particularly distressing.
- Pupils with social, emotional or mental health needs, where excessive or harmful online use may compound existing vulnerabilities.
- Looked-after children and previously looked-after children.

Before any lesson covering sensitive online safety content, the class teacher will consider whether any pupil may have lived experience of the topic and, in consultation with the DSL, will plan to provide appropriate support without drawing attention to individual pupils.

5. Educating parents and carers about online safety

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

Online safety will also be covered during the welcome parents' evenings in the Autumn term, curriculum information events and, where appropriate, dedicated parent workshops.

The school will let parents and 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.
- Practical steps parents can take to keep children safe at home, including parental controls and family conversations about online life.

If parents or 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.

6. Cyber-bullying and online harm

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. (See also the school Behaviour Policy.)

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 encourage them 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 — as part of our PSHE and computing curriculum and through assemblies. Class teachers will discuss cyber-bullying with their classes when relevant.

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, especially PTA, (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11).

The school also shares information with parents and carers so they are aware of the signs of cyber-bullying, 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 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.

6.3 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 or DSL.
- Explain to the pupil why they are being searched, and 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 for the staff member in conjunction with the DSL or headteacher 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 whether there is a good reason to erase data or files from a device, staff members will consider whether 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 or 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 deputy DSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UKCIS guidance on sharing nudes and semi-nudes.

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.
- Our Behaviour Policy.

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

6.4 Artificial intelligence (AI)

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

St Wilfrid's CE Primary Academy recognises that AI has many uses to help pupils learn and to reduce avoidable staff workload, but it also carries risks. These include the creation of 'deepfakes' — images, audio or video hoaxes that look real — and deepfake pornography, where AI is used to create pornographic content incorporating someone's likeness. AI tools can also hallucinate (produce false information presented as fact), reflect bias, or surface harmful content.

The school will treat any use of AI to bully, harass or harm pupils very seriously, in line with our Behaviour Policy and Child Protection and Safeguarding Policy.

All use of artificial intelligence by staff and pupils is governed by the school's separate AI Policy, which sits alongside this Online Safety Policy and should be read in conjunction with it. The AI Policy sets out:

- The approved AI tools that staff may use (with Microsoft Copilot as the preferred tool, Google NotebookLM and Gamma are also approved for specific purposes).
- The 'golden data rule' — no identifiable information about any member of the St Wilfrid's community may be entered into any open AI tool, and first-name use is only permitted within tools where staff are signed into the school's tenancy.
- The six core rules for responsible AI use: fair, transparent, safe and reliable, secure and private, sustainable, and accountable.
- The position on pupil use of AI — pupils do not currently have independent access to generative AI tools; all pupil-facing use is mediated by an adult.
- The role of the Digital Leadership Team in approving new AI tools, maintaining the AI Risk Register, and overseeing AI use in practice.

Staff are aware of the risks of using AI tools while they are still being developed. Any new AI tool proposed for use in the school must be approved by the Digital Leadership Team in advance, following a risk assessment that considers safeguarding, data protection and curriculum impact. Existing AI tools are reviewed annually.

Any safeguarding concern arising from the use of AI — whether by staff, pupils or others — is logged on CPOMS and managed in line with the school's Child Protection and Safeguarding Policy. Any suspected data breach involving AI is reported to the Data Protection Officer in line with the Data Protection Policy.

6.5 Child-on-child sexual abuse and online harassment

All staff understand that pupils may be less likely to report concerning online sexual behaviours, especially where they have been using age-inappropriate sites or platforms. Staff must recognise the indicators of online harmful sexual behaviour, which include:

- Threatening, facilitating or encouraging sexual violence.
- Sexualised online bullying, such as sexual jokes, taunts or sustained name-calling.
- Unwanted and unsolicited sexual comments, messages or images.
- Consensual or non-consensual sharing of sexualised imagery, including nudes and semi-nudes.
- Abuse between young people in intimate relationships online.
- Upskirting — taking a picture underneath a person's clothing without consent (an offence under the Voyeurism (Offences) Act 2019).

Staff promote zero tolerance for sexual harassment or abuse and challenge any attempts by pupils to minimise or normalise such behaviour. Staff are aware that creating, possessing or sharing indecent images of anyone under 18 is a criminal offence, including where the imagery is created or shared by the child depicted themselves.

All concerns about online child-on-child sexual abuse or harassment are reported to the DSL without delay and managed in line with the school's Child Protection and Safeguarding Policy, regardless of where or how the incident occurred.

6.6 Grooming, exploitation and contact risks

Grooming describes the situation in which an adult, or in some cases an older child, builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting or abusing them. Grooming often takes place online and pupils who are being groomed are commonly unlikely to report this behaviour, due to feelings of loyalty, fear, distress or confusion.

Staff are alert to the indicators of online grooming, which may include:

- A pupil being secretive about how they are spending their time online.
- A pupil having an older online 'friend' or 'partner' whom their family and friends have not met.
- A pupil having money, new possessions or gifts that they cannot or will not explain.
- Sudden changes in mood, withdrawal, or unexplained anxiety related to device use.

Staff also understand the online dimensions of:

- **Child sexual exploitation (CSE)** — including sexual coercion online and grooming into wider exploitation networks.
- **Child criminal exploitation (CCE)** — including children being recruited online into county lines drug transportation, shoplifting and serious violence.

Any concern about grooming, CSE or CCE is reported to the DSL without delay and managed in line with the school's Child Protection and Safeguarding Policy.

6.7 Radicalisation and extremism

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies. Extremist groups use social media and other online platforms to identify, target and recruit vulnerable individuals.

Staff exercise vigilance towards any pupils displaying indicators that they may have been, or are being, radicalised. Concerns are reported to the DSL without delay and handled in line with the school's Prevent Duty obligations and Child Protection and Safeguarding Policy.

6.8 Harmful online challenges and online hoaxes

For the purposes of this policy:

- **An online hoax** is a deliberate lie spread online, usually to scare or distress.
- **A harmful online challenge** is a social media trend in which participants record and share videos of themselves performing an action. A challenge becomes harmful if it risks physical or emotional harm, either directly or through how the content is shared.

Where staff suspect that a harmful online challenge or hoax is circulating amongst pupils, they will report this to the DSL immediately. The DSL will assess each case individually to determine the nature and scale of risk.

Before deciding how to respond, the DSL and headteacher will weigh whether each proposed response is:

- In line with advice from a known, reliable source (for example the UK Safer Internet Centre).
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge when they would not otherwise have come across it.
- Proportional to the actual or perceived risk.
- Appropriate for the relevant pupils' age and developmental stage.
- In line with the Child Protection and Safeguarding Policy.

A school-wide response will only be used where the risk of increasing exposure has been carefully considered and mitigated.

6.9 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories:

- **Cyber-enabled crime** — offences that can be carried out offline but are made easier or larger in scale by use of the internet (for example fraud, the purchase and sale of illegal items, and elements of sexual abuse and exploitation).
- **Cyber-dependent crime** — offences that can only be carried out online or using a computer (for example illegal hacking, making or supplying malware, and 'booting' attacks).

The school is alert to the risk that pupils with a particular skill or affinity for technology may become involved, deliberately or inadvertently, in cyber-crime. Where staff have concerns about a pupil's use of technology and their intentions, the DSL will consider whether a referral to the National Crime Agency's Cyber Choices programme is appropriate. Cyber Choices supports children who are at risk of committing cyber-crime and helps redirect them to positive uses of their skills.

The school's curriculum supports pupils to use technology safely, responsibly and lawfully.

7. Acceptable use of the internet in school

7.1 General principles

All pupils, parents and 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, where 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.

The school will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above, and restricts access through filtering systems where appropriate. Active monitoring is carried out via Securus, with alerts reviewed by the DSL.

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

7.2 PTA, hirers, contractors and visitors

The school's Wi-Fi and ICT facilities are extended to a range of non-staff users on a controlled basis. The arrangements below apply:

- **The Parents and Teachers Association (PTA)** — PTA members and volunteers using the school's Wi-Fi or ICT systems while on premises (for example, to support school events, fundraising activities or PTA meetings held on site) are bound by the acceptable use terms set out in Appendix 3. The PTA Chair or designated representative is responsible for ensuring that PTA members and volunteers understand these terms. PTA use of the school's Wi-Fi is for PTA-related activity only and accessed via a one day only code obtained via the school office.
- **Lettings and hirers** — where school premises are hired by external groups (for example, community groups, sports clubs or external providers running out-of-hours provision), hirers do not receive access to the school's main Wi-Fi network. Any ICT-related arrangements for hirers are set out in the lettings agreement and must be approved in advance by the School Business Manager.
- **Visitors and contractors** — visitors and contractors who require internet access on premises are issued a 24-hour guest Wi-Fi code on request from the school office. The guest code provides time-limited, filtered access on a network segregated from the school's main systems. Guest users are expected to use the connection responsibly and in line with the principles set out in Appendix 3; the school reserves the right to revoke guest access at any time.
- **Governors** — when on premises, governors use the 24-hour guest Wi-Fi code on request from the school office and are bound by the acceptable use agreement at Appendix 3.

All users of the school's Wi-Fi — main network or guest network — are subject to the school's filtering arrangements. The guest Wi-Fi is filtered and monitored separately from the staff and pupil networks, with appropriate content restrictions in place. Any attempts to bypass filtering, or any use that gives rise to safeguarding concerns, will be investigated by the DSL in line with this policy.

8. Pupils using mobile devices in school

Pupils in Years 5 and 6 may bring mobile devices into school but are not permitted to use them on the school premises during the school day. Devices must be switched off and stored in the secure class mobile phone lockers.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (Appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour Policy, which may result in the confiscation of their device. Confiscation will be carried out in accordance with section 6.3 of this policy.

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 — strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager.
- Ensuring their hard drive is encrypted — this means that 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 promptly 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.

If staff have any concerns about the security of their device, they must seek advice from the headteacher in the first instance, who will liaise with Entrust as required.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in its Behaviour Policy and the ICT and internet acceptable use agreement. 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 school's staff disciplinary procedures and the Trust's 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. Where appropriate, the school will also report content directly to the Internet Watch Foundation (IWF), the Child Exploitation and Online Protection (CEOP) command, or other relevant authorities.

The school will not criminalise pupils for inadvertent or curiosity-driven behaviour. In all cases the DSL and headteacher will ensure that the needs of the child are placed before the needs or reputation of the school.

11. Training

11.1 Staff, governors and volunteers

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, threatening, harassing and misogynistic messages; non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups; and the sharing of abusive images and pornography with those who do not 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.
- Understand their expectations, roles and responsibilities relating to filtering and monitoring systems.

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every two 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 the school's Child Protection and Safeguarding Policy.

12. Monitoring arrangements

The DSL logs all behaviour and safeguarding issues related to online safety on CPOMS.

In addition, the school maintains a separate online safety incident log (Excel) to record alerts generated by the Securus filtering and monitoring system that do not, in themselves, constitute a safeguarding concern but which inform the school's understanding of patterns and trends — for example, repeated low-level filtering breaches by particular year groups. Where any such alert escalates into a safeguarding concern, it is also logged on CPOMS in line with section 3.3.

The DSL reviews the online safety incident log at least termly to identify patterns and any gaps in provision, and uses this data to update procedures and inform staff training.

This policy will be reviewed annually by the Headteacher. 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.

13. Links with other policies

This Online Safety Policy is linked to the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy

- AI Policy
- Prevent Duty Policy
- PSHE Policy
- Relationships and Health Education Policy

Appendix 1: EYFS and KS1 acceptable use agreement

(For 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 use the computers 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 choose a website by mistake, get messages from people I don't know, or find anything that may upset or harm me or my friends. • Use school computers for schoolwork 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 number) to anyone without the permission of my teacher or parent or carer. • Save my work on the school network. • Check with my teacher before I print anything. • Log off or shut down a computer or other device 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/carers 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

(For 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 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 or 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 have 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 or 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, 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 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

(For staff, governors, volunteers, the PTA, visitors and contractors using the school's ICT systems or Wi-Fi)

Acceptable use of the school's ICT systems, Wi-Fi and internet: agreement for staff, governors, volunteers, the PTA, visitors and contractors

Name:

Role / capacity (please tick): ☐ Staff ☐ Governor ☐
Volunteer ☐ PTA ☐ Visitor ☐ Contractor

When using the school's ICT systems, the school's Wi-Fi (including the guest Wi-Fi), or 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 that could harm the school's reputation.
- Access social networking sites or chat rooms for non-professional purposes.
- 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 the headteacher or DSL first.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I am not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.
- Enter personal or sensitive data into generative AI tools (see the school's AI Policy).

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 DSL and ICT service provider know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will use any generative AI tools in line with the school's AI Policy and this Online Safety Policy.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed:

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 (including Securus)?	
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?	
Do you know how to log an online safety incident on CPOMS?	
Are you familiar with the school's AI Policy?	
Are there any areas of online safety in which you would like training/further training?	