Online Safety Policy

Approved by	Richard McCabe
Approval date	July 2026 (effective 1 September 2026); revised November 2026
Next review due	August 2027
Applies to	All registered pupils aged 7–16, staff, volunteers and visitors at Grovehill and Gaddesden
Document status	Final
Proprietor/chair signature	

Related policies

Behaviour Policy
Child Protection and Safeguarding Policy
Staff Code of Conduct Policy
Complaints and Compliments Policy

Contents

1. Aims....4
2. Legislation and guidance....4
3. Roles and responsibilities....5
3.1 The proprietor/chair....5
3.2 The Headteacher....5
3.3 The designated safeguarding lead (DSL)....5
3.4 IT contractors....6
3.5 All staff and volunteers....6
3.6 Parents/carers....7
3.7 Visitors and members of the community....7
4. Educating pupils about online safety....7
4.1 Pupils will be taught about online safety as part of the curriculum....7
Across the curriculum....9
4.2 Pupils will be taught practical cyber security skills....9
5. Educating parents/carers about online safety....10
6. Cyber-bullying....10
6.1 Definition....10
6.2 Preventing and addressing cyber-bullying....10
6.3 Examining electronic devices....11
6.4 Artificial intelligence (AI)....12
7. Acceptable use of the internet in school....13
8. Pupils using mobile devices in school....13
9. Staff using work devices outside school....14
10. How the school will respond to issues of misuse....14
11. Training for staff, governance members and volunteers....14
12. Monitoring arrangements....15
13. Links with other policies....15
Appendix 1: Acceptable use agreement (pupils and parents/carers)....16
Appendix 2: acceptable use agreement (staff, governance members, volunteers and visitors)....17
Appendix 3: online safety training needs – self-audit for staff....18

1. Aims

Safety, Empathy and Ambition guide this policy: pupils are protected from harm, supported without blame to seek help, and taught in accessible, developmentally appropriate ways that build independence.
Our school aims to:

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

The 4 key categories of risk

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

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

2. Legislation and guidance

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

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying, including cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education; Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. It also reflects current DfE searching, screening and confiscation guidance: only the Headteacher, or a staff member they have expressly authorised, may search a pupil or examine a confiscated device, and any examination, deletion or transfer must meet the guidance's legal tests and safeguarding controls.

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

This policy has been prepared in accordance with the Independent School Standards and the school's proprietor and governance arrangements.

3. Roles and responsibilities

3.1 The proprietor/chair

The proprietor/chair has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation at Grovehill and Gaddesden.

The proprietor/chair will make sure all staff undergo online safety training as part of child protection and safeguarding training, and understand their roles and responsibilities for filtering and monitoring.

The proprietor/chair will also make sure all staff receive regular online safety updates, as required and at least annually, so that they retain the skills and knowledge needed to safeguard pupils effectively.

The proprietor/chair will receive regular assurance from the designated safeguarding lead (DSL) and the Headteacher on online safety incidents, training needs, filtering and monitoring effectiveness, and agreed actions.

The proprietor/chair will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The proprietor/chair provides strategic assurance that appropriate filtering and monitoring systems are in place and effective. The Headteacher is the named internal SLT owner at Grovehill and Gaddesden; the DSL leads on safeguarding effectiveness and response; and IT contractors provide technical operation, configuration, change records and evidence under school instructions. The annual review will use the DfE's filtering and monitoring standards and will 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

Any governance members supporting the proprietor/chair will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that teaching about safeguarding, including online safety, is individually adapted for every Redbourn Park pupil. Teaching will reflect communication and AAC needs, sensory profiles, developmental starting points, EHCP outcomes, lived experience and the online risks actually encountered; a one-size-fits-all approach is not appropriate

3.2 The Headteacher

The Headteacher is responsible for making sure staff understand this policy and implement it consistently at Grovehill and Gaddesden. The Headteacher is the internal SLT owner for filtering and monitoring and owns the school's operational use and administration of Earwig and Google Classroom.

3.3 The designated safeguarding lead (DSL)

The Headteacher, site leads and senior teachers are the deputy designated safeguarding leads (DDSLs), as set out in the Child Protection and Safeguarding Policy and relevant job descriptions.

The DSL takes lead responsibility for the safeguarding aspects of online safety across both sites, including CPOMS practice and safeguarding decisions. In particular, the DSL is responsible for:

- Supporting the Headteacher in making sure staff understand this policy and implement it consistently at both sites
- Working with the Headteacher and the proprietor/chair to review this policy annually and keep its procedures and implementation current
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing the proprietor/chair and the Headteacher with safeguarding assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with IT contractors on technical evidence while retaining safeguarding decision-making within the school
- Working with the Headteacher, IT contractors and other staff as necessary to address online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that online safety incidents are recorded on CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains the staff online safety training-needs self-audit)
- Liaising with other agencies and/or external services if necessary
- Providing regular online safety reports to the Headteacher and the proprietor/chair
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 IT contractors

IT contractors act only within the scope of their contract and school instructions. They provide technical implementation, configuration, security, filtering and monitoring evidence, and change logs; they do not make safeguarding, policy or disciplinary decisions. Their responsibilities are:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Carrying out security checks and system monitoring in accordance with the contract and a risk-based schedule, and retaining evidence of material configuration changes
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Escalating technical faults, alerts and suspected online safety incidents immediately to the Headteacher and the DSL, and supplying technical evidence; IT contractors do not determine the safeguarding or disciplinary response
- Supporting the school with technical containment and evidence where requested; safeguarding and behaviour decisions remain with school leaders

This list is not intended to be exhaustive.

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 staff acceptable use agreement in appendix 2, and making sure pupils follow the pupil acceptable use agreement in appendix 1
- Understanding the filtering and monitoring responsibilities: the Headteacher is the internal SLT owner; the DSL owns safeguarding assessment and CPOMS practice; IT contractors provide technical operation; and the proprietor/chair provides strategic assurance. A failure must be reported immediately to the Headteacher and the DSL and recorded on CPOMS. Any temporary educational bypass must be documented and authorised by the Headteacher, implemented by IT contractors, and discussed with the DSL where a safeguarding risk may arise; the purpose, scope, duration and reversal must be logged
- Working with the DSL to make sure online safety incidents are recorded on CPOMS and dealt with appropriately in line with this policy
- Report cyber-bullying and online-safety concerns immediately to the DSL and a DDSL; record safeguarding concerns on CPOMS and follow the Behaviour Policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff, the Headteacher or the DSL of any concerns or queries regarding this policy
- Make sure their child has been supported to understand and agree to the pupil acceptable use agreement in appendix 1

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

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

3.7 Visitors and members of the community

Visitors and community members who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. Where relevant, they will agree to the acceptable use terms in appendix 2.

4. Educating pupils about online safety

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

Redbourn Park teaches the relevant statutory relationships, sex and health education content across its 7–16 provision. Content is selected and sequenced from each pupil's assessed starting point rather than assumed age or key-stage attainment, and includes:

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

For pupils working from early developmental starting points, teaching will include:

- 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

As pupils develop the readiness to apply broader online-safety concepts, teaching will include:

- 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

As relevant knowledge and independence develop, these themes will be extended and revisited through a spiral curriculum:

- 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
- Before pupils are supported to use an online platform, staff will check its current terms, minimum-age rules, consent requirements and safety settings; no single fixed age is assumed across services. Teaching will explain how age restrictions and privacy controls can reduce exposure to inappropriate content and unsafe contact
- 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 pictures or words have been circulated, they may be impossible to remove everywhere and the pupil may lose control over where they appear
- 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

Where a pupil's development, communication and digital experience make more complex outcomes appropriate, teaching will include:

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

Across Redbourn Park's 7–16 provision, the following content will be selected and adapted to each pupil's communication and AAC needs, sensory profile, EHCP outcomes, assessed understanding and the online risks they actually encounter:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images

- Pupils will be taught, in a non-blaming and developmentally appropriate way, that creating, keeping or forwarding a sexual image of someone under 18 may be a criminal offence, including where the image is self-generated, consensual or AI-generated, and that sharing an intimate image of an adult without consent may also be an offence. Teaching will emphasise help-seeking rather than threats of punishment: a pupil will not be in trouble for asking for help and should tell a trusted adult immediately. The DSL will lead the safeguarding response and involve the police where necessary and proportionate
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

Across the curriculum

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

All online-safety teaching will be individually adapted because every Redbourn Park pupil has SEND. Adaptations will reflect communication and AAC needs, sensory profiles, developmental starting points, EHCP outcomes, lived experience and the risks encountered online.

4.2 Pupils will be taught practical cyber security skills

All 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 cyberbullying and the risks of online radicalisation.

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 virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

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

Parents/carers should raise online safety queries or concerns with the Headteacher and/or the DSL.

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

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. (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 discuss cyber-bullying with pupils in accessible, non-blaming language, including why it occurs, the forms it may take, its impact and how to seek help. Staff will teach and reinforce this during lessons and individual or group sessions, including through personal, social, health and economic (PSHE) education and other relevant curriculum areas.

All staff, governance members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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

If the DSL has reasonable grounds to suspect that material is illegal, the DSL will secure the device and any evidence unchanged, seek police advice promptly and follow police directions for preservation and transfer. Staff will not view, copy, print, store or forward suspected intimate images or other illegal material and will work with external services where necessary.

6.3 Examining electronic devices

The Headteacher, and only a named member of staff expressly authorised by the Headteacher, may search for and confiscate an electronic device where there are reasonable grounds to suspect 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

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

- Assess the urgency and the risk to the pupil, other pupils and staff. If the search is not urgent, seek advice from the Headteacher and the 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 or suspected, staff will secure the device unchanged and notify the DSL and the Headteacher. The DSL will lead the safeguarding decision, consulting the Headteacher and police where necessary. Staff must not examine suspected intimate images and must not view, copy, print, store or forward them.

Before erasing any data or file, staff will consider whether it may be evidence of an offence. Suspected evidence must not be deleted, altered or copied; the device will be secured unchanged and police advice sought, with transfer carried out as directed. If the material is not suspected evidence and deletion is otherwise lawful under the DfE guidance, staff may delete it only if:

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

If a staff member suspects a device may contain a nude or semi-nude image of a child, including an AI-generated or manipulated image, they will:

- Not view, copy, print, store, forward or otherwise reproduce the image
- Secure the device unchanged and report the incident immediately to the DSL and the Headteacher. The DSL will decide the safeguarding response in line with the DfE's latest searching, screening and confiscation guidance and the UKCIS guidance on sharing nudes and semi-nudes, seeking police advice where required

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The Behaviour 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)

Only school-approved AI tools may be used for school activity, through managed school accounts where available. Before use, the school will check current provider terms, minimum-age requirements, consent requirements and account controls.

AI may support learning and accessibility, but it can also create inaccurate, biased or harmful output and be used for bullying, impersonation and deepfakes, including sexually explicit content using a person's likeness.

Harmful output, unsafe use, AI-enabled bullying or suspected sexual imagery must be reported immediately to the DSL and recorded on CPOMS. The school will respond under the Behaviour Policy and Child Protection and Safeguarding Policy.

Before introducing a new AI tool or a new high-risk use, the school will complete a proportionate risk assessment and, where personal data, special-category data or systematic monitoring is involved, a data protection impact assessment. AI output must be checked by a competent human before it informs teaching, assessment, safeguarding or operational decisions, and accessibility and reasonable adjustments must be considered.

Staff and pupils must not enter personal, safeguarding, special-category or confidential information into an AI service unless that specific use has written school approval, appropriate contractual and data-protection safeguards, and any required data protection impact assessment. All AI use must comply with the AI Usage Policy.

7. Acceptable use of the internet in school

All pupils and parents/carers are expected to complete the pupil acceptable use agreement in appendix 1. Staff, governance members, volunteers and relevant visitors must complete the agreement in appendix 2.

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.

Filtering and monitoring will cover school networks and school-managed devices on site and, where management controls allow, school-managed devices used off site. Monitoring will be transparent, necessary and proportionate to safeguarding and security purposes. Access to monitoring data will be limited to authorised staff and IT contractors acting under school instructions; data will be retained and deleted under the approved retention schedule. Urgent alerts will be routed directly to the Headteacher and the DSL, with CPOMS used for the safeguarding record. A risk assessment and, where required, a data protection impact assessment will be completed before new or high-risk monitoring is introduced.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Redbourn Park is phone-free by default during the school day. A pupil who brings a phone to school must hand it to the Headteacher, or a person they delegate, on arrival. The Headteacher will ensure it is placed in secure, individually identified storage and that receipt, authorised access and return are logged.

The Headteacher may approve and document an individual exception for medical, disability, communication or AAC, regulation, transport or emergency needs. If a pupil does not hand over a phone, staff will respond calmly, assess immediate risk and involve the pupil, the Headteacher and family as appropriate. Refusal will not by itself trigger automatic separation; any search or confiscation must be lawful, necessary, proportionate and consistent with the Behaviour Policy.

A pupil may carry a phone on journeys to and from school where this is consistent with their individual plan. Unless an approved exception applies, the phone must be handed to the Headteacher, or a person they delegate, on arrival and returned through the logged process at departure.

Pupils may not use mobile phones, except under a documented individual exception, in:

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

Any use of a mobile device in school by a pupil must comply with the pupil acceptable use agreement in appendix 1 and any documented individual plan.

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.

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 3 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 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 a device in any way that would breach the staff acceptable use agreement in appendix 2.

Work devices must be used solely for work activities.

Staff must report device-security concerns immediately to the Headteacher and IT contractors, and notify the DSL where safeguarding information may be affected.

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 Behaviour Policy and the relevant Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the 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 Disciplinary Policy in the Staff Handbook and the Staff Code of Conduct Policy. 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.

11. Training for staff, governance members 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 nude and semi-nude images and/or videos, including AI-generated or manipulated imagery, especially in chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

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

The proprietor/chair and any governance members supporting them will receive training on safe internet use and online safeguarding as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL ensures that online-safety safeguarding concerns, decisions and outcomes are recorded on CPOMS. The DDSLs ensure prompt local action and direct escalation.

This policy will be reviewed annually by the DSL with the Headteacher. The proprietor/chair will approve it at every review. The review will include the annual filtering and monitoring effectiveness check and a risk assessment reflecting the online risks pupils actually face, recognising that technology, risks and harms change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Handbook (Disciplinary Policy)
- Data Protection Policy
- Complaints and Compliments Policy
- Acceptable use agreements (appendices 1 and 2)

Appendix 1: 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:	
This agreement will be explained in an accessible way, using Easy Read, symbols, AAC or adult-supported discussion where needed. I will be supported to show that I understand and agree to follow these rules. 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 trusted adult immediately if I find anything that might upset, distress or harm me or someone else ■ 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 a staff member has expressly allowed this as part of an approved learning activity ■ Open any attachments in emails, or follow any links in emails, without first checking with a member of staff ■ Use any inappropriate language when communicating online, including in emails ■ Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate ■ Log in to the school's network using someone else's details ■ Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: ■ I will not use it during lessons, tutor-group time, clubs or other activities organised by the school without permission from the staff member leading the activity ■ 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 2: acceptable use agreement (staff, governance members, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNANCE MEMBERS, VOLUNTEERS AND VISITORS	
Name of staff member/governance member/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ■ Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ■ Use them in any way that could harm the school's reputation ■ Access social networking or chat services unless the service, account and work purpose have been formally approved and safeguarding and data-protection controls are in place ■ 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 unless I am authorised to do so and use only an approved school device, account and service; I will never use a personal device or account ■ Share confidential information about the school, its pupils or staff, or other members of the community ■ Access, modify or share data I'm not authorised to access, modify or share ■ Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will notify the DSL and a DDSL immediately if a pupil reports, or I encounter, material that may upset, distress or harm them or others, and I will record the safeguarding concern on CPOMS. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governance member/volunteer/visitor):	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, governance members 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 use a long, unique password for each school system, use multi-factor authentication where available, and change a password promptly if it may have been compromised?	
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?	