

Online Safety

Procedures & Policy

Avenue House School



Approved by:

Last reviewed on: September 2026

Next review due by: September 2027

*As this document will be shared with all school staff on the first INSET day (1 September 2026), the **[Updated]** reference has been left in place to highlight amendments made since the previous version.*

Contents:

[Updated] [Statement of intent](#)

1. **[Updated]** [Legal framework](#)
2. **[Updated]** [Roles and responsibilities](#)
3. **[Updated]** [Managing online safety](#)
4. [Cyberbullying](#)
5. **[Updated]** [Child-on-child sexual abuse and harassment](#)
6. **[Updated]** [Grooming and exploitation](#)
7. **[Updated]** [Mental health](#)
8. **[Updated]** [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. **[Updated]** [Online safety and the curriculum](#)
12. **[Updated]** [Use of technology in the classroom](#)
13. **[Updated]** [Use of mobile devices](#)
14. **[Updated]** [Educating parents](#)
15. [Internet access](#)
16. **[Updated]** [Filtering and monitoring online activity](#)
17. [Network security](#)
18. **[Updated]** [Emails](#)
19. **[Updated]** [Artificial intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

Statement of intent

Avenue House School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful content, e.g. pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories.
- **Contact:** Being subjected to harmful online interaction with other users or generative AI applications that simulate this, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Online behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit images, including those generated using AI and online bullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Children's wellbeing and schools Act 2026
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education'
- DfE 'Teaching online safety in schools'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence (AI) in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Technology Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy

- Mobile Devices Policy
- Code of Conduct for Staff, Governors and Volunteers
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Photography and Images Policy
- Device User Agreement
- Prevent Duty Policy
- **[New]** Safe Use of AI Policy

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an **annual** basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security Policy.

[Updated] The **DSL, Justin Sheppard & DDSL- Ravinder Nandra**, will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the **SENCO- Rahat Malik and ICT technician- Brent Maytham**

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- **[Updated]** Understanding the filtering and monitoring processes in place at the school and ensuring they continue to meet the school's safeguarding needs.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Working with the headteacher and ICT technicians to conduct termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.

[Updated] All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.

- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- **[Updated]** Having an awareness of current and emerging online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement 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. **[Updated]** Managing online safety

[Updated] All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people. Staff will understand that pupils are at risk of abuse and other safeguarding concerns online as well as face to face, and in many cases, abuse will take place concurrently online and offline.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive annual training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation

- Online safety is integrated into learning throughout the curriculum– At the start of the year in ICT, in the PSHE curriculum and Safer Internet Day each year. (This is the minimum)
- Assemblies are conducted termly on the topic of remaining safe online

[Updated] Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

[Updated] The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. where a pupil has shared nudes or semi-nudes of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response will be recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. **[Updated]** Child-on-child sexual abuse and harassment

[Updated] Pupils may use the internet and technology to facilitate child-on-child sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, offline and online, and that online elements may facilitate or accompany abuse that also occurs face to face.

[Updated] The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- **[Updated]** Consensual or non-consensual making or sharing of nudes and semi-nudes, including those generated or altered using AI.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

[Updated] Staff will be aware that creating, possessing, and distributing nudes or semi-nudes involving other children, including images generated or altered using AI may constitute a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves. Such incidents will be handled in accordance with the Making or Sharing of Nude or Semi-nude Images Policy.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy, Child Protection and Safeguarding Policy, and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. [Updated] Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

[Updated] Child sexual exploitation (CSE) and child criminal exploitation (CCE)

[Updated] Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways online. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production or distribution of child sexual abuse material (CSAM), or the sexual exploitation and trafficking of children.

[Updated] CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting (including county lines activity), shoplifting, serious violence and other forms of criminal exploitation. While these crimes

often take place in person, it is increasingly common for children to be groomed and manipulated into participating online.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

7. [Updated] Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand apps, games and websites, online terminology, the ways in which social interactions online in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Wellbeing & Mental Health Policy, to Rahat Malik.

8. **[Updated]** Online hoaxes and harmful online challenges

For the purposes of this policy, an “**online hoax**” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online, e.g. via social media, game chats, and messaging platforms.

For the purposes of this policy, “**harmful online challenges**” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video online, e.g. through social media channels, and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

[Updated] Where staff become aware of, or suspect, a harmful online challenge or online hoax that may pose a risk to pupils, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.

- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

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

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

Through The National College and training in-house, the DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate

abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. [Updated] Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE & Citizenship
- ICT & Safer Internet Day like events

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

[Updated] Content risks

[Updated] Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as AI-generated content, deepfakes, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

[Updated] Contact risks

[Updated] The school will educate pupils about the potential dangers of interacting with others online or generative AI applications that simulate this. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

[Updated] Conduct risks

[Updated] Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with making, sharing or receiving nudes and semi-nudes, including images that have been generated or altered using AI. Online bullying, including the use online platforms, e.g. social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their

personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and DSL will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. **[Updated]** Use of technology in the classroom

Technology used during lessons, may include the following:

- Laptops
- Cameras

[Updated] Prior to using any websites, tools, apps, AI systems or other online platforms in the classroom, or recommending that pupils use these platforms at home, the teacher will review and evaluate the resource to ensure it is appropriate, safe and suitable for the age and needs of the pupils. Teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision will be suitable to their age and ability.

13. **[Updated]** Use of mobile devices

While the school recognises that the use of mobile devices can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

[New] Pupils will not be permitted to use personal mobile devices at any point during the school day unless exceptions apply

Staff will use all personal technology in line with the school's Staff ICT and Electronic Devices Policy.

[Updated] The school recognises that pupils may have access to the internet through personal devices and mobile phone networks outside the school day, or where school restrictions are circumvented. This can increase the risk of online behaviour that places pupils at risk of harm and breaches the school's Mobile Devices Policy and Technology Acceptable Use Agreement for Pupils.

[New] Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the Behaviour Policy.

[Updated] Inappropriate use of smart technology may include:

- Using mobile devices to sexually harass, bully, troll or intimidate peers.

- **[Updated]** Making or sharing nudes and semi-nudes, including images generated or altered using AI, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of technology and outline the importance of using technology in an appropriate manner.

[Updated] The school will seek to ensure that it remains up to date with emerging technologies, including AI tools, devices, platforms, apps, trends and related risks.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. **[Updated]** Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

[Updated] Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- **[Updated]** Making or sharing nudes and semi-nudes, including images generated or altered using AI.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Newsletters
- Parent Information Meeting

15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the **school office**.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. **[Updated]** Filtering and monitoring online activity- with Securly

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

[New] The school will do all it reasonably can to limit pupils' exposure to online risks from the school's ICT system. The school will put in place appropriate filtering and monitoring systems and ensure that their effectiveness is reviewed at least annually and whenever there is a significant change to the school's network, safeguarding risks or technology provision. Reviews will be carried out by the SLT member responsible for filtering and monitoring with support from the DSL and ICT technicians.

[New] Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school

implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by Brent Maytham. Firewalls will be always switched on and will be reviewed on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to the DSL, Headteacher and the ICT Technician.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils from Year 1 and above will be provided with their own unique username and private passwords. Staff members and pupils in KS2 will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Staff will inform ICT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber-security Policy.

18. [Updated] Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and Staff and Volunteer Confidentiality Policy.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement.

Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

[Updated] Staff members and pupils will be required to block spam and junk mail and report the email to the DSL and ICT technicians. The school's monitoring system Securly, can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians will organise annual cyber awareness training, including guidance on recognising phishing emails, AI-generated phishing attempts and other malicious communications. This training will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. **[Updated]** Artificial intelligence (AI)

[Updated] The school will take steps to prepare pupils for changing and emerging technologies, including generative AI, and teach them how to use AI safely, responsibly and appropriately, taking account of their age and developmental stage.

The school will ensure its ICT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal, confidential or sensitive information is not entered into AI tools unless this is authorised, secure and compliant with data protection legislation. Children will not have access to AI tools- sites be blocked through Securly.

[New] Where staff use AI tools to support teaching, learning or administrative tasks, they will do so in accordance with the school's Safe Use of AI Policy and DfE guidance on generative AI in education.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

21. The school website

The headteacher will be responsible for the overall content of the school website – she will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

22. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

23. Remote learning

All remote learning will be delivered in line with the school's Remote Education statement in the Curriculum Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on an **annual** basis and following any online safety incidents.

.

Any changes made to this policy are communicated to all members of the school community.

Appendix A- Related Online Resources

- Keeping Children Safe in Education (KCSIE)
- Meeting digital and technology standards in schools and colleges
- Data Protection in schools
- The Prevent Duty

London Grid for Learning (LGfL) <https://lgfl.net/TypesOfHarm/OnlineSafetyAudit>

Southwest Grid for Learning (SWGfL) <https://360safe.org.uk/>

- Cyber security training for school staff
- UK Safer Internet Centre <https://saferinternet.org.uk/>
- Digital Resilience <https://www.headstartkernow.org.uk/digital-resilience/>

Appendix B – Acceptable Use of ICT Form EYFS & KS1

My Digital Safety Promise

Acceptable use of the school's ICT systems, devices and internet

When I use the school's computers, tablets, cameras, other technology and the internet, I will:

- Only use technology when a teacher or trusted adult says I can.
- Use websites, apps and games that a teacher has chosen or approved.
- Ask for help if I am unsure about anything online.
- Tell a teacher or trusted adult straight away if:
 - I see something that worries, upsets or confuses me.
 - I have received a message I do not understand.
 - I accidentally visit a website I should not be on.
- Be kind and respectful to everyone when using technology.
- Use technology to help me learn.
- Look after school equipment and tell an adult if something is broken, damaged or not working properly.
- Keep my username and password private.
- Never use another person's account or password.
- Never share personal information about me or others online, including names, addresses, photographs, telephone numbers or passwords, unless a teacher says it is safe to do so.
- Only take photographs, videos or recordings when a teacher has given permission.
- Check with a teacher before printing or downloading anything.
- Log off or close programs properly when I have finished using a device.
- Remember that not everything online is true and ask a trusted adult if I am unsure.
- Only use online tools, including AI tools, when a teacher has authorised their use.

School Monitoring

I understand that the school checks and monitors the use of school devices, systems and internet access to help keep everyone safe.

My Promise

When using computers, tablets, cameras and the internet I promise to:

☒ Be Safe

☒ Tell an Adult if I am Worried

☒ Be Kind

☒ Be Responsible

Signed (pupil):

Date:

Parent/Carer Agreement

I have read and discussed this agreement with my child.

I understand that:

- The school takes reasonable steps to help keep pupils safe when using technology.
- The school uses filtering and monitoring systems to support online safety.
- My child's use of school ICT systems, devices and internet access may be monitored when using school equipment, accounts or networks.
- Pupils are expected to follow the school's online safety and acceptable use expectations.
- I will support the school by encouraging my child to use technology safely, responsibly and respectfully.
- I will encourage my child to tell a trusted adult if they encounter anything online that worries, upsets or confuses them.

Signed (parent):

Date:

Appendix C – Acceptable Use of ICT Form KS2

Acceptable Use of the School's ICT Systems, Devices and Internet

Pupil Agreement

When using the school's computers, tablets, devices, network, internet and online services, I understand that I am responsible for using them safely, respectfully and responsibly.

I agree to:

Staying Safe Online

- Use the internet and digital technologies for learning and educational purposes as directed by school staff.
- Tell a teacher or trusted adult immediately if:
 - I see anything online that makes me feel uncomfortable, worried or unsafe.
 - I receive a message or communication that upsets me or seems inappropriate.
 - I accidentally access unsuitable content.
- Remember that people online may not always be who they say they are.
- Check information I find online and ask an adult if I am unsure whether it is accurate or trustworthy.
- Only use online services, websites or apps approved by the school.

Respecting Others

- Be polite, kind and respectful when using technology.
- Always use appropriate language.
- Treat others online in the same way I would expect to be treated.
- Never use technology to bully, upset, exclude, threaten or embarrass anyone.
- Report any concerns about online bullying or unkind behaviour to a member of staff.

Protecting Personal Information

- Keep my username and password secret.
- Never use another person's account or attempt to access information that does not belong to me.
- Never share personal information about me or others online, including:
 - home addresses
 - telephone numbers
 - email addresses
 - passwords
 - photographs or videos
- Ask a teacher before sharing any information online.

Using School Equipment Responsibly

- Look after school devices and equipment carefully.
- Report any damage, faults or concerns immediately.
- Only use equipment and software provided or approved by the school.
- Not change settings or install software without permission.
- Log off or lock devices when I have finished using them.
- Print only when instructed to do so.

Digital Content and Copyright

- Use information, images and media responsibly.
- Acknowledge sources when required.
- Not copy the work of others and pretend it is my own.

- Respect copyright and intellectual property rights.

Use of Artificial Intelligence (AI)

- Only use AI tools when authorised by a teacher.
- Use AI-generated content responsibly.
- Never submit AI-generated work as entirely my own unless instructed that this is acceptable.
- Tell a teacher if I am unsure whether an AI tool can be used for a piece of work.

Personal Devices

Where permitted by the school:

- Use personal devices in accordance with school rules.
- Not use personal devices to photograph, film or record others without permission.
- Understand that personal devices may be restricted during the school day.

Monitoring and Filtering

I understand that:

- The school uses filtering and monitoring systems to help keep pupils safe.
- My use of school devices, systems, internet access and online services may be monitored.
- The school may investigate concerns relating to the misuse of technology.

Pupil Declaration

I understand this agreement and will use technology safely, responsibly and respectfully.

Signed (pupil):

Date:

Parent Agreement

As the parent of the pupil named above, I understand that:

- The school provides access to technology and internet services to support learning.
- The school uses filtering and monitoring systems to help protect pupils online.
- Reasonable monitoring may take place when school devices, accounts, networks or systems are used.
- Pupils must follow the school's acceptable use, safeguarding and behaviour expectations.
- The school cannot guarantee that all online risks can be eliminated but takes reasonable steps to reduce them.
- I will support the school's online safety approach and encourage responsible technology use at home.

I/We agree to:

- Discuss safe and responsible technology use with my child.
- Encourage my child to tell a trusted adult if they experience anything online that causes concern.
- Work in partnership with the school to address any online safety concerns.
- Support the school's expectations regarding the use of school systems, online services and personal devices.

Signed (parent):

Date:

Appendix D – Acceptable Use of ICT Form- Staff

Acceptable Use of ICT Systems, Digital Technologies and Internet Services

Introduction

The school provides access to ICT systems, digital devices, networks, online services and internet resources to support teaching, learning and the effective operation of the school.

This agreement applies to all staff, governors, volunteers, agency staff, contractors and any other individuals authorised to access the school's ICT systems.

All users are expected to use technology safely, professionally, responsibly and in accordance with statutory requirements, including safeguarding and data protection legislation, and the school's policies and procedures.

Professional Use of Technology

I will:

- Use school ICT systems primarily for educational and professional purposes.
- Demonstrate professional conduct and good digital citizenship at all times.
- Model safe, responsible and respectful technology use for pupils.
- Maintain the reputation of the school when using digital technologies.
- Follow all relevant school policies and procedures.

I will not:

- Use school systems for unlawful, offensive, inappropriate or discriminatory purposes.
- Access, create, store or share inappropriate material using school systems.
- Use school technology in a manner that may bring the school into disrepute.

Safeguarding Responsibilities

I recognise that safeguarding is everyone's responsibility.

I will:

- Support the school's safeguarding culture through safe and appropriate use of technology.
- Report immediately any online safety or safeguarding concern involving a pupil.
- Report any concerning online behaviour, content or communication to the Designated Safeguarding Lead (DSL).

- Maintain appropriate professional boundaries in all online communications.
- Ensure digital resources used with pupils are suitable and age appropriate.
- Follow school procedures when using online learning platforms and communication systems.

I will not:

- Communicate with pupils through personal email accounts, social media accounts or personal messaging applications.
- Establish inappropriate online relationships with pupils.
- Share or access material that may place pupils or colleagues at risk.

Data Protection and Confidentiality

I understand my responsibilities under data protection legislation.

I will:

- Access personal data only where required for my professional duties.
- Handle personal and sensitive information securely and confidentially.
- Ensure confidential information is only shared with authorised individuals.
- Take appropriate precautions when sending information electronically.
- Store personal information securely.
- Report actual or suspected data breaches immediately in accordance with school procedures.

I will not:

- Share confidential information with unauthorised individuals.
- Remove or transfer personal data to unauthorised systems, applications or storage locations.
- Leave confidential information visible on unattended devices.

Passwords and Account Security

I will:

- Keep usernames, passwords and authentication credentials secure.
- Use strong passwords and multi-factor authentication where available.
- Lock or log out of devices whenever they are left unattended.
- Report suspected security breaches immediately.

I will not:

- Share passwords or login credentials.

- Allow another person to use my account.
- Attempt to gain unauthorised access to systems, files or accounts.

Use of School Devices, Systems and Networks

I will:

- Take reasonable care of school equipment.
- Use only authorised software, systems and applications.
- Report faults, damage or technical issues promptly.
- Follow school expectations for remote and hybrid working.
- Ensure devices are kept secure when used off-site.

I will not:

- Install software without authorisation.
- Connect unauthorised equipment to the school's network.
- Circumvent security controls, filtering systems or monitoring arrangements.
- Use school systems in a way that may compromise security, performance or safeguarding.

Email, Communication and Collaboration Platforms

I will:

- Use school-approved communication systems for school business.
- Communicate professionally and respectfully.
- Check recipients carefully before sending emails or documents.
- Exercise caution when opening attachments or following links.

I will not:

- Send offensive, inappropriate or discriminatory communications.
- Forward chain messages, spam or malicious content.
- Use personal email accounts to conduct school business unless authorised.

Social Media and Online Conduct

I understand that my online activity can affect my professional reputation and that of the school.

I will:

- Follow the school's Social Media Policy and Staff Code of Conduct.
- Maintain appropriate professional boundaries online.
- Act responsibly when publishing or sharing online content.

I will not:

- Share confidential school information online.
- Discuss pupils, parents/carers or colleagues on social media.
- Publish content that may damage the reputation of the school or undermine public confidence in my professional role.

Artificial Intelligence (AI)

Where AI tools are authorised for educational or administrative use, I will:

- Use AI responsibly, ethically and professionally.
- Check and verify the accuracy of AI-generated content before use.
- Exercise professional judgement when using AI outputs.
- Ensure pupils are supervised appropriately when using AI tools.
- Follow any school guidance relating to the use of AI technologies.

I will not:

- Enter confidential, sensitive or personal data into AI systems unless specifically authorised by the school.
- Present AI-generated content as wholly my own professional work without appropriate review.
- Rely solely on AI-generated information when making professional decisions.

Filtering, Monitoring and Cyber Security

I understand that the school uses Securly filtering and monitoring systems to help safeguard pupils, staff and visitors.

I acknowledge that:

- Securly filtering and monitoring operates on the school's devices, network and internet services.
- Activity on school ICT systems may be monitored where lawful, proportionate and appropriate.
- Safeguarding alerts generated through Securly may be reviewed by authorised staff, including safeguarding and senior leaders.
- Monitoring helps support safeguarding, wellbeing, cyber security and compliance with school policies.

- Deliberately attempting to bypass filtering, monitoring or security systems is strictly prohibited.
- Suspected misuse of school technology may result in investigation and disciplinary action.

I will:

- Use school systems in a manner consistent with safeguarding expectations.
- Cooperate with any investigation relating to technology use where required.
- Report any concerns regarding filtering, monitoring or cyber security controls.

Personal Devices

Where personal devices are authorised for school use, I will:

- Follow the school's Bring Your Own Device (BYOD) procedures.
- Ensure personal devices used for school purposes are protected with passwords and security updates.
- Take appropriate steps to protect school information stored or accessed on personal devices.

I will not:

- Store sensitive school information on personal devices without authorisation.
- Use personal devices in ways that compromise safeguarding, data protection or cyber security.

Declaration

I confirm that I have read, understood and agree to comply with this Acceptable Use Agreement and all associated school policies.

I understand that failure to comply with this agreement may result in the withdrawal of ICT access, disciplinary action and, where appropriate, referral to external agencies.

Name:	Date:
Signed:	

Appendix E – Acceptable Use of ICT Form– Governors

Acceptable Use of ICT Systems, Digital Technologies and Information

Introduction

As a Governor, I recognise that I have access to confidential information and play an important role in supporting the school's strategic leadership, safeguarding arrangements and governance responsibilities.

I understand that I must use information and communication technology (ICT) systems, digital services and information responsibly, securely and in accordance with relevant legislation and school policies.

This agreement applies whenever I access school systems, information, networks, devices, email accounts, governor portals or cloud-based services, whether on school premises or remotely.

Governance Responsibilities

I will:

- Support the school's commitment to safeguarding, online safety, information security and data protection.
- Behave professionally and ethically when using digital technologies.
- Use information obtained through my role solely for governance purposes.
- Comply with all relevant school policies and procedures.
- Protect the reputation of the school when using digital technologies and online platforms.

I will not:

- Use school systems for personal, commercial, political or unlawful purposes.
- Share information obtained through my governance role without appropriate authority.
- Access information beyond that required for my governance responsibilities.

Confidentiality and Information Governance

I understand that governors may have access to highly sensitive information regarding pupils, staff, finances and school operations.

I will:

- Maintain confidentiality at all times.
- Handle and store confidential information securely.
- Ensure papers and documents are protected from unauthorised access.

- Dispose of confidential information securely when no longer required.
- Follow the school's data protection procedures.

I will not:

- Discuss confidential matters in public places or with unauthorised individuals.
- Forward confidential documents to personal accounts unless authorised and appropriately secured.
- Retain confidential information longer than necessary.

Data Protection

I understand my responsibilities under UK data protection legislation.

I will:

- Access personal data only when required to fulfil my governance role.
- Use personal data fairly, lawfully and securely.
- Take appropriate steps to prevent unauthorised disclosure of information.
- Report any actual or suspected data breach immediately to the school.

I will not:

- Download, copy or share personal data unnecessarily.
- Store sensitive information in unsecured locations.
- Transfer school information to unauthorised systems or applications.

Passwords and Account Security

I will:

- Keep passwords confidential and secure.
- Use strong passwords and multi-factor authentication where available.
- Ensure devices used to access school information are appropriately protected.
- Log out of systems when access is complete.
- Report any suspected security incident immediately.

I will not:

- Share login credentials with anyone.
- Use another person's account.
- Allow unauthorised access to governor accounts or school systems.

Email and Electronic Communications

I will:

- Use school-provided email accounts and systems for governance-related business wherever possible.
- Check recipients carefully before sending information.
- Take care when sending confidential documentation electronically.
- Remain vigilant against phishing emails, scams and cyber security threats.

I will not:

- Forward confidential information to unauthorised recipients.
 - Open suspicious links or attachments where legitimacy cannot be verified.
 - Use school communication systems for inappropriate purposes.
-

Remote Access and Personal Devices

Where I use personal devices to access school information, I will:

- Ensure devices are password protected and appropriately secured.
- Keep operating systems and security software up to date.
- Store information securely and remove it when no longer required.
- Prevent family members or other individuals from accessing confidential school information.

I will not:

- Access school information using unsecured public devices.
 - Save confidential documents in unsecured locations.
 - Leave devices containing school information unattended in public places.
-

Safeguarding

As a Governor, I recognise my responsibilities for safeguarding and promoting the welfare of children.

I will:

- Report any safeguarding concerns immediately in accordance with school procedures.
- Handle safeguarding information with the highest level of confidentiality.
- Follow the school's safeguarding and child protection policies.
- Support the school's approach to online safety and digital safeguarding.

I will not:

- Share safeguarding information with anyone who does not have a legitimate need to know.
- Retain safeguarding records unnecessarily.

Social Media and Online Conduct

I will:

- Act professionally when using social media and online platforms.
- Be mindful that online activity may affect the reputation of the school.
- Maintain appropriate boundaries when discussing school-related matters online.

I will not:

- Identify or discuss pupils, parents/carers or staff on social media.
- Share confidential or sensitive information online.
- Publish material likely to bring the school into disrepute.

Artificial Intelligence (AI)

Where AI tools are used in support of governance activities, I will:

- Use AI responsibly and professionally.
- Verify the accuracy of AI-generated content.
- Apply my own judgement when reviewing AI outputs.
- Ensure confidential, personal or safeguarding information is not entered into AI systems unless explicitly authorised by the school.

I understand that responsibility for decisions remains with me and cannot be delegated to an AI tool.

Filtering, Monitoring and Cyber Security

I understand that the school uses **Securly** filtering and monitoring systems to support safeguarding, cyber security and the safe use of technology.

I acknowledge that:

- Access to school systems and networks may be monitored where lawful, proportionate and appropriate.
- Monitoring and filtering arrangements support the school's safeguarding responsibilities.
- Any suspected misuse of school systems may be investigated.

- Deliberately attempting to bypass security, filtering or monitoring controls is prohibited.

I will:

- Follow all cyber security requirements communicated by the school.
- Report suspected cyber security incidents immediately.
- Cooperate with investigations where necessary.

Declaration

I confirm that I have read, understood and agree to comply with this Acceptable Use Agreement.

I understand that failure to comply with this agreement may result in the withdrawal of access to school systems and information and may be reported to the Governing Board and relevant authorities where appropriate.

Governor Name:

Signed:

Date:

Appendix F – Acceptable Use of ICT Form- Volunteers & Visitors

Visitor, Volunteer and Temporary User Acceptable Use Agreement Acceptable Use of ICT Systems, Devices and Internet Services

Introduction

The school provides access to ICT systems, devices, networks, internet services and digital resources to support learning and the effective operation of the school.

This agreement applies to all visitors, volunteers, contractors, trainees, supply staff, students on placement and other individuals who may be granted access to the school's ICT systems, devices, network or guest wireless services.

All users are expected to use technology safely, responsibly and in a manner that supports the school's safeguarding responsibilities.

Safeguarding Responsibilities

I understand that safeguarding and promoting the welfare of children is everyone's responsibility.

I will:

- Support the school's safeguarding and online safety arrangements.
- Report immediately any safeguarding concerns to a member of school staff.
- Follow all instructions provided regarding the safe use of technology.
- Maintain appropriate professional boundaries at all times.
- Use school technology and internet services appropriately.

I will not:

- Access, display, create or share inappropriate material.
- Use school systems in a manner that could place pupils or staff at risk.
- Communicate electronically with pupils unless specifically authorised and supervised by the school.

Use of School Systems and Internet Access

I will:

- Use school ICT systems, devices and internet access only for authorised purposes.
- Follow instructions provided by school staff regarding the use of equipment and digital services.

- Take reasonable care of any equipment provided to me.
- Log out of systems when I have finished using them.

I will not:

- Attempt to access information, files or systems without permission.
- Install software or applications on school devices.
- Attempt to bypass security controls, filtering or monitoring systems.
- Access websites or services that are inappropriate or unrelated to my authorised activities.

Confidentiality and Data Protection

During my visit or voluntary work, I may become aware of confidential information relating to pupils, staff or the school.

I will:

- Treat all information obtained through my role as confidential.
- Follow any instructions given regarding data protection and confidentiality.
- Immediately report any concerns about the security of information.

I will not:

- Share confidential information with unauthorised individuals.
- Take photographs, screenshots, recordings or copies of information without permission.
- Retain school information after my authorised access has ended.

Passwords and Security

Where access credentials are provided, I will:

- Keep usernames and passwords secure.
- Use only the account provided to me.
- Report any suspected security issue immediately.

I will not:

- Share passwords or login details.
- Allow another person to use my account.
- Attempt to gain unauthorised access to systems or information.

Personal Devices

Where authorised to use a personal device on school premises, I will:

- Follow the school's expectations regarding personal device use.
- Keep my device secure and protected by a password or PIN.
- Use personal devices responsibly and appropriately.

I will not:

- Photograph, film or record pupils, staff or visitors without permission.
- Access or store confidential school information on personal devices unless authorised.
- Use personal devices in a way that compromises safeguarding or data protection.

Filtering and Monitoring

I understand that the school uses **Securly** filtering and monitoring systems to support safeguarding, online safety and cyber security.

I acknowledge that:

- Internet access and use of school systems may be monitored where lawful and appropriate.
- Filtering and monitoring systems help protect pupils, staff and visitors.
- Any attempts to bypass filtering, monitoring or security systems are prohibited.
- Suspected misuse of school technology may be investigated.

Acceptable Online Behaviour

I will:

- Use respectful and appropriate language in any electronic communication.
- Act professionally and responsibly when using school technology.
- Respect the rights, privacy and wellbeing of others.

I will not:

- Access, create, transmit or store offensive, discriminatory or inappropriate content.
- Engage in cyberbullying, harassment or any form of online abuse.
- Use school systems for unlawful activities.

Declaration

I confirm that I have read, understood and agree to comply with this Acceptable Use Agreement.

I understand that failure to comply may result in the withdrawal of access to school ICT systems and, where appropriate, referral to the relevant authorities.

Visitor / Volunteer / Temporary User

Name: _____

Organisation (if applicable): _____

Signed:

Date: