WEST HATCH HIGH SCHOOL

THE BEST THAT I CAN BE

Online Safety Policy

Policy Date	October 2026
Policy to be reviewed	October 2027

Signed by the Headteacher

Ratified on the by the Chair of Governors

Signed:

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in school 8
8. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training ..... **Error! Bookmark not defined.**
12. Monitoring arrangements 11
13. Links with other policies 11
Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers) 12
Appendix 2: acceptable use agreement (staff, governors and volunteers) 13

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, report, 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, racism, misogyny/misandry, self-harm, suicide, antisemitism, 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 human interaction, 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** – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, including images generated or altered using AI, deepfakes, online bullying and other abusive or discriminatory behaviour; 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 2026, and current guidance and standards for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (statutory guidance in force from 1 September 2026)
- Searching, screening and confiscation
- Mobile phones in schools (statutory guidance, 2026)
- Plan technology for your school
- Education for a Connected World
- Filtering and monitoring: core standard for schools and colleges (updated September 2026)
- Cyber security: core standard for schools and colleges (updated September 2026)
- Harmful online challenges and online hoaxes
- Generative AI: product safety standards
- Generative artificial intelligence (AI) in education and DfE safe-use support materials
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Prevent duty guidance

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, the Education Act 2011, the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025. The Education Act 2011

gives teachers powers, where the statutory conditions are met, to search for and delete inappropriate images or files on pupils' electronic devices where there is a good reason to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

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

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks. A review of the effectiveness of the provision will be carried out at least once every academic year by the SLT member responsible for filtering and monitoring, supported by the DSL and Network Manager/IT support. The review will include checks that filtering is working appropriately on all internet-connected school-managed devices and in all relevant locations, and a record of checks and resulting actions will be kept. The board will review the DfE filtering and monitoring standards and discuss with school leaders, IT staff and service providers what further action is required.

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provision at least once every academic year and recording the review, checks and resulting actions
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs
- Considering whether filtering and monitoring can appropriately manage real-time, dynamic, personalised and AI-generated content, taking account of the school's pupil risk profile

The governing board will also seek assurance that appropriate cyber security measures and procedures are in place as part of the school's wider safeguarding responsibilities, with regard to the DfE cyber security core standard.

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 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, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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

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

The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Supporting the annual filtering and monitoring review with the responsible SLT member and Network Manager/IT support, reviewing relevant reports and ensuring concerns are escalated and acted upon appropriately
- Making sure that any online safety incidents are logged on MyConcern 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks 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 The Network Manager
The Network Manager is responsible for:
- Putting in place and maintaining appropriate security, filtering and monitoring systems on school devices and school networks, including consideration of real-time, dynamic, personalised and AI-generated content. The systems will be reviewed at least once every academic year and following significant changes to technology, software, working practices or identified safeguarding risks

- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Supporting the school's annual cyber security risk assessment and termly review of cyber risks, and implementing actions arising from identified vulnerabilities or incidents
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

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 terms on acceptable use of the school's ICT systems and the internet (appendix 2), and making sure that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Reporting filtering, monitoring or cyber-security concerns promptly and not attempting to disable, bypass or circumvent the school's security, filtering or monitoring controls
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could and does happen here'.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

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

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

- CEOP Child exploitation and Online Protection
- Childnet
- Parentzone
- Internet Matters
- NSPCC
- Thinkuknow
- UK Safer Internet Centre

3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

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

The text below reflects the National Curriculum computing programmes of study and the revised statutory Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance, which came into force on 1 September 2026.

All schools have to teach:
- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **KS3**, pupils will be taught to:
- 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

Pupils in **KS4** will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That keeping, forwarding, acquiring or generating indecent or sexual images of someone under 18 is illegal, including where an image has been created or altered using AI, and how to seek help if an image has been shared
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

- How social media can contain fake or AI-generated accounts and content, and how to critically evaluate online relationships and sources of information
- About the prevalence of deepfakes, including images and videos, how they may be used maliciously, the harms they can cause and how to identify and report them
- How technology and social media can be used as part of bullying, harassment, stalking, coercive and controlling behaviour, and how to seek support
- About online scams and financially motivated sexual extortion (sextortion), how to recognise these risks and where to seek help
- That AI chatbots and other emerging technologies can create simulated relationships or fake intimacy and may provide harmful or misleading advice, and the importance of critical thinking and seeking support from trusted adults

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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. This policy will also be shared with parents/carers. Online safety will also be covered during parents' evenings.

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy).

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups and addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices (see the DfE Searching, Screening and Confiscation guidance)

Please refer to Appendix 9 of the Behaviour policy

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and can create or alter text, images, audio and video, as well as simulate human interaction. Staff and pupils may encounter these tools both within approved educational products and through publicly available services.

West Hatch recognises that AI can support teaching and learning but can also create safeguarding risks. These include AI-generated or altered sexual imagery, deepfakes, impersonation, bullying, misinformation, harmful or manipulative content, simulated relationships or fake intimacy, and tools that provide unsafe or misleading advice.

West Hatch will treat any use of AI to bully pupils very seriously, in line with our Behaviour policy. Before a new AI tool is introduced, or an existing tool is used in a new way, the school will consider the safeguarding, filtering and monitoring, data protection, security, intellectual property, age-appropriateness and SEND implications. Where appropriate, a risk assessment will be completed and the DfE Generative AI: product safety standards will be considered.

Staff and pupils must only use AI tools in accordance with school approval and policy. Personal, confidential or safeguarding information must not be entered into unapproved AI services. Any safeguarding concern arising from AI use must be reported immediately in the same way as any other safeguarding concern.

Any use of artificial intelligence should be carried out in accordance with our AI Policy.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 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.

We will monitor online activity on school-managed devices and networks, where appropriate and lawful, to support safeguarding and cyber security. Access will be restricted through filtering systems where appropriate. Users must not attempt to bypass, disable or circumvent the school's filtering, monitoring or security controls.

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

8. 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
- Using multi-factor authentication where it is provided or required and keeping authentication codes secure

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, suspect a cyber incident or data breach, or lose a school device, they must report this promptly to the ICT manager and follow the school's data-protection and incident-reporting procedures.

9. Mobile phones and personal devices

In line with the DfE statutory guidance on mobile phones in schools, West Hatch High School is a phone-free environment. Pupils should not have access to or use mobile phones during the school day, including lessons, movement between lessons, breaktimes and lunchtimes, except where a specific authorised exception or reasonable adjustment applies. Detailed expectations, storage arrangements, exceptions and consequences are set out in the school's Behaviour Policy and/or Mobile Phone Policy. The school will keep the safeguarding implications of personal devices under review as technology develops.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the school's disciplinary procedures. 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, safeguarding concerns, serious misuse, AI-generated harmful content or a cyber-security incident should be reported or referred to the Police, Children's Social Care, the LADO, the school's Data Protection Officer and/or other relevant agencies, as appropriate to the circumstances.

11. Training

11.1 Staff, Governors and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

Online safety training will include the school's filtering and monitoring arrangements, the responsibilities of staff in relation to those systems, how to report and escalate concerns, cyber-security awareness, and emerging risks associated with generative AI.

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, racist, discriminatory, misogynistic or misandrist messages
    - Non-consensual making or sharing of nude and semi-nude images and/or videos, including content generated or altered using AI, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Generative AI can create safeguarding risks, including deepfakes, AI-generated sexual imagery, impersonation, harmful advice and simulated interactions, and staff must know how to identify and report concerns

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

11.2 Pupils

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
- How to recognise and report deepfakes, AI-generated harmful content and other manipulated media
- How to use approved AI tools safely, critically and responsibly and where to seek help if an AI interaction causes concern
- How to recognise online scams, grooming and sextortion and how to report concerns

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via MyConcern.

This policy will be reviewed annually by the DSL and updated sooner where statutory guidance, technology or the school's risk profile changes. The review will be supported by an annual online-safety risk assessment that considers the risks pupils face. The effectiveness of filtering and monitoring will be reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, with the DSL and Network Manager/IT support and involvement of the responsible governor. Checks will include school-managed internet-connected devices and relevant locations, and a record of checks and resulting actions will be kept. Additional review will take place where a safeguarding risk is identified, new technology or generative-AI tools are introduced, major software or network changes occur, or working practices change. The school will also complete an annual cyber-security risk assessment and revisit cyber risks during the year.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Behaviour policy
- Mobile Phone Policy
- Relationships and Sex Education Policy
- AI Policy
- Staff Disciplinary Procedures
- Data Protection policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use policy

Appendix 1: Pupil Acceptable Use Agreement (this agreement appears on the screen when students first log in for them to sign)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Name of Pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is 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 **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:**

Appendix 2: Acceptable Use Agreement (staff, governors and volunteers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer:
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 sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
When using generative AI, I will use only school-approved tools, follow the school's AI and data-protection requirements, and will not enter confidential, personal or safeguarding information into an unapproved AI service. When using generative AI, I will use only school-approved tools, follow the school's AI and data-protection requirements, and will not enter confidential, personal or safeguarding information into an unapproved AI service. I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**