Online Safety Policy

Approved by: Full Governing Board **Date:** September 2026

Next review due by: September 2027

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 6
5. Educating parents about online safety 7
6. Cyber-bullying 7
7. Artificial Intelligence (AI)..... 8
8. Prevention of Radicalisation and Extremism.....8
9. Acceptable use of the internet in school 9
10. Pupils using mobile devices in school 10
11. Staff using work devices outside school 10
12. How the school will respond to issues of misuse 10
13. Training 11
14. Monitoring and Filtering arrangements.....11
15. Links with other policies 12
Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers) 13
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 14

1. Aims

Implementation of our School Values –

- Respect
- Kindness
- Resilience
- Curiosity
- Friendship

The Reigate School expectations require all children to ensure they are Ready, Respectful and Safe.Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for Behaviour, Safeguarding, Anti-bullying and Staff Code of Conduct. This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization, 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 with generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, including those generated using AI (e.g. consensual and non-consensual sharing of nudes and semi- nudes and/or pornography), sharing other explicit images and online bullying;
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation and Guidance

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

- Teaching online safety in schools
- Relationship and Sex Education
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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 Safeguarding Governor will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing the whole school approach to safeguarding and related policies and procedures including filtering and monitoring.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and/deputies 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 ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Filtering and Monitoring of online content
- Working with the Headteacher 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 child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour & Rewards 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

This list is not intended to be exhaustive.

3.4 Virtual IT

Virtual IT are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are raised with the DSL team so incidents are dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour & Rewards 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 ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with school policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour & Rewards Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents and Carers

Parents and carers are expected to:

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

Parents and carers can seek further guidance on keeping children safe online via the school website safeguarding section and from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to

the terms on acceptable use (appendix 2).

4. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum through the PSHE tutor time programme and Life Skills lessons. Where opportunities in the wider curriculum present themselves, staff will educate students about the topic of online safety.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education in secondary schools

In **Key Stage 3**, 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 **Key Stage 4** 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 AI and deepfake awareness and 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 which 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 sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online, recognising how algorithms shape online feeds
- How to identify harmful behaviours online (including bullying, abuse or harassment, misogyny, incel culture, addictive online interests) 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 safe use of social media and the internet will also be covered in other subjects where relevant (eg

Life Skills)

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 About Online Safety

The school will raise parents' and carers' awareness of online safety via the school newsletter and other communications home, as well as information via our school website safeguarding section. This policy will also be shared with parents and carers.

Online safety will also be covered during specific information evenings for parents' and carers'.

If parents and carers have any queries or concerns in relation to their child's online safety, these should be raised in the first instance with the relevant pastoral team or 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged 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 as part of the safeguarding tutor time programme

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (Life Skills) 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 12 for more detail).

The school also sends information on cyber-bullying to parents so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or

other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that is a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on

Searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance of sharing nudes and semi-nudes: advice for education settings working with children and young people

* *Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

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

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

7. Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils, parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft CoPilot or Google Gemini.

Reigate School recognises there are benefits and risks to children using AI and staff, parents/carers should risk assess any tools being used by children either in school or at home. Risks can include deepfakes where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography; pornographic content created using AI to include someone's likeness.

Reigate School will treat any use of AI to bully a child in line with the school's behaviour policy.

8. Prevention of Radicalisation and Extremism

In order to promote a safe and secure online learning environment, we are committed to implementing a comprehensive online safety policy that aligns with the Prevent Duty. Our paramount objective is to safeguard students and staff against the risk associated with online activities, ensuring the all members of our school community are aware and equipped to respond to potential threats. The Prevent Duty obliges us to counteract the risk of radicalization and extremism, and our online safety policy plays a crucial role in fulfilling this obligation.

8.1 Introduction

The purpose of this section is to outline the measures and strategies implemented by Reigate School to prevent radicalisation and extremism amongst pupils, ensuring a safe online environment conducive to learning in line with our Prevent Duty.

Definition

For the purpose of this policy, "radicalisation" refers to the process by which an individual is exposed to and adopts extremist ideologies, leading to a willingness to support or engage in activities promoting violence or harm.

8.2 Objectives

- Early Detection: Identify signs of radicalization or extremist behavior among pupils.
- Prevention: Implement measures to prevent radicalisation of pupils.
- Education: Equip pupils with the knowledge and critical thinking skills to discern extremist content online.

8.3 Implementation Strategies

Integrate awareness and education about radicalisation and extremism into the school curriculum to foster critical thinking, digital literacy and ethical behavior.

Training and Awareness Programs

- Staff training:
  - Annual safeguarding refresher training
  - Annual Prevent training
  - Staff briefings and safeguarding updates
- Pupil Awareness:
  - Age appropriate assemblies and activities though the Tutor Time and Life Skills curriculum to educate pupils about the dangers of online radicalisation and the importance of responsible behaviour online.

Implement a robust online monitoring and filtering system (see section 13) to identify and restrict access to extremist content.

Any concerns of radicalisation or extremist views must be reported to the DSL (or deputies) and Headteacher. The incident will be recorded on the pupil's electronic safeguarding file via CPOMS.

The DSL and Headteacher will assess the incident and either:

- Respond with internal processes where there is no identified safeguarding risk/pattern of behavior or
- Refer to Prevent and complete a national referral form in line with statutory guidance

8.4 Evaluation and Review

Reigate School has a robust Prevent risk assessment and each term the DSL and Headteacher assess the effectiveness of prevention measures and make adjustments as necessary. Review and update this policy annually to align with emerging online threats and education needs including updates in Keeping Children Safe in Education and any other statutory guidance.

8.5 Conclusion

Reigate School is committed to a providing safe and secure online environment for all pupils. By implementing proactive measures to prevent radicalisation and extremism, we aim to foster a culture of respect, tolerance and critical thinking which are in line with the fundamental British Values.

9. Acceptable Use of the Internet in School

All pupils, parents, carers, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, Governors and visitors (where relevant) to ensure they comply with the above.

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

10. Pupils Using Mobile Devices in School

Reigate School implements a Not Seen, Not Heard policy to mobile phones. Pupils who have a mobile device to support their travel to/from school are not permitted to use them during:

- Lessons
- Tutor group time
- Break or Lunch
- On site clubs (before or after school) or any activities organised by the school

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

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour and Rewards Policy, which may result in the confiscation of their device.

11. 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 – always install the latest updates

Staff members must not use the device in any way which 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, they must seek advice from the Virtual IT/school IT Helpdesk

12. How the School will Respond to Issues of Misuse

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

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, 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

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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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.

14. Monitoring and Filtering Arrangements

Reigate School provides a safe environment to learn and work, including when online. Monitoring and Filtering are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

At Reigate School we use Securus Software to ensure we have robust systems in place and Securus has been at the forefront of providing online safeguarding solutions to schools for many years. By developing leading edge solutions designed to safeguard young people against online dangers they helped pioneer the concept of online safety.

Staff and pupils are aware of the monitoring and filtering provision and understand what information is captured when using the school network (either in school or remotely). Each school computer has a Securus log-in screen to remind pupils and staff about acceptable usage and school expectations when accessing content online.

All captures are shared with the DSL and Headteacher with appropriate follow-up and sanctions where necessary. The DSL/deputies log safeguarding issues related to online safety on CPOMS. Behaviour online violations are recorded on Arbor.

This policy will be reviewed every year by the DSL and Headteacher. At every review, the policy will be shared with the Governing Board. The review will be supported by an annual monitoring and filtering risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Rewards Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only **Consent to the school's Securus monitoring & filtering log-in screen and understand that any inappropriate capture will be shared with the DSL, Headteacher and other relevant staff for further follow-up in line with school policies.**
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username 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 which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm 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
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, lunch time, break time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
 Staff, governors, volunteers and visitors are expected to consent to the school's Securus monitoring & filtering log-in screen and understand that any inappropriate capture will be shared with the DSL, Headteacher for further follow-up in line with school policies. **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 which 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 teacher's 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	
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 which 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 - abide by the acceptable use agreement and the expectations detailed in the school's behavior and online safety policy.	
Signed (staff member/governor/volunteer/visitor):	**Date:**