Dallas Road Community Primary School



Online Safety Policy 2026

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, including mobile and smart technology (which we refer to as 'mobile phones').

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. LEGISLATION & GUIDANCE

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

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff [Relationships and sex education (RSE) and health education

Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. 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 considers the National Curriculum computing programmes of study.

3. ROLES AND RESPONSIBILITIES

3.1 The governing body

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 governor who oversees online safety is Ines Cotarelo. As the nominated governor she will hold regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Online Safety Lead and designated safeguarding lead (DSL).

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 Online Safety Lead and Designated Safeguarding Lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and

service providers what needs to be done to support the school in meeting those standards, which include:

Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.

Reviewing filtering and monitoring provisions at least annually.

Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.

Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

Ensure 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.

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.

Ensure 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 contextualized 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 designated safeguarding lead (DSL) and Deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Working with the governing board to review this policy annually and ensure 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 Deputy DSLs, 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

Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy.

Responding to safeguarding concerns identified by filtering and monitoring

Ensuring 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 governing board

Regularly consider and reflect on the risks children face.

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Technical Staff

Under guidance from the DSL, the external technical support employed by the school are responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated at least annually 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.

Regularly conducting a full security check and monitoring the school's ICT systems.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this 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 and ensuring that pupils follow the school's terms on acceptable use (See Appendices).

Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by notifying the school technical staff and reporting on CPOMS.

Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with the safeguarding policy.

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here.'

This list is not intended to be exhaustive.

3.6 Parents

Parents 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 (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from a variety of organisations and websites found on the school website:

https://www.dallasroad.lancs.sch.uk/Online-Safety/

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.

4. EDUCATING PUPILS

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

National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for teaching until 31 August 2026).

All schools must teach:

Relationships education and health education in primary schools

In Key Stage (KS) 1, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private.

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage (KS) 2 will be taught to:

Use technology safely, respectfully and responsibly.

Recognise acceptable and unacceptable behaviour.

Identify a range of ways to report concerns about content and contact.

Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.

People sometimes behave differently online, including pretending to be someone they are not.

That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.

The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.

How information and data are shared and used online.

How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.

What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.

Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online.

How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.

Where and how to report concerns and get support with issues online.

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. The Computing Policy sets out a focus of e-safety for each half term this will be shared through lessons, displays and assemblies. Additionally, staff will be responsive in educating pupils if a specific issue arises within the class.

5. EDUCATING PARENTS & CARERS

The school will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website and school communication tools such as Arbor,

This policy will also be shared with parents.

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 using.

If parents 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. CYBERBULLYING

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.

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 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 safeguarding and behaviour policies. Where illegal, inappropriate or harmful material

has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices.

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or

Is identified in the school rules as a banned item for which a search can be carried out, and/or Is evidence in relation to an offence.

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

Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from DSL.

Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.

Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should suspect that the device has, or could be used to:

Cause harm, and/or

Undermine the safe environment of the school or disrupt teaching, and/or

Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/headteacher to decide on a suitable response. If there are images, data or files on the device that staff suspect is likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice on education settings working with children and young people.

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

The DfE's latest guidance on searching, screening and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Our behaviour policy

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

6.4 Artificial intelligence (AI)

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

Dallas Road recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of '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.

Dallas Road will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where

existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. ACCEPTABLE USE IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

Visitors can use the "Dallas Road Guest' Network via a secure password.

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.

8. PERSONAL MOBILE DEVICES, SMART WATCHES AND OTHER WEARABLE TECHNOLOGY IN SCHOOL

Pupils may bring mobile phones into school when they are in Year 6 but are not permitted to use them during the school day. If a child requires a mobile phone, this is handed to a member of staff at the start of the day and collected at home time. Smart watches and other personal wearable technology are not permitted unless agreed by the HT or member of SLT.

Staff may use their own mobile phone and smart watch in school during social time (away from pupils) or in emergency situations.

Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers) as does the liability for any loss or damage.

See Mobile Phone Policy for more details.

9. STAFF USING WORK DEVICES OUT OF 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, using a strong password.

Making sure the device locks if left inactive for a period.

Not sharing the device among family or friends

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. Staff are also required to sign a device loan agreement for any school devices assigned specifically to them such as iPad or Macbook (appendix 4).

If staff have any concerns over the security of their device, they must seek advice from the school technical support.

10. COMMUNICATION

The school uses several online methods of communication. These include Parent App, SeeSaw, Showbie, Arbor, email and Facebook. Staff should only use assigned methods when contacting parents or pupils. When contacting parents via email or phone staff should do this through school methods or by withholding their number when using their own phone. This is to ensure the personal contact details of staff are not shared.

11. SOCIAL MEDIA

As part of the computing curriculum, pupils will learn about the risks and benefits to social media as well as the age restrictions for using specific social media platforms. Pupil iPads will be restricted to block the use of social media within school.

Staff who choose to make use of social networking site/media should be advised as follows: -

(i) That they familiarise themselves with the site's 'privacy settings' to ensure that information is not automatically shared with a wider audience than intended.

(ii) Engage fully in any training offered in relation to online safety and use of social media.

(iii)That they do not conduct or portray themselves in a manner which may: - bring the school into disrepute. lead to valid parental complaints. be deemed as derogatory towards the school and/or its employees. be deemed as derogatory towards pupils and/or parents and carers. bring into question their appropriateness to work with children and young people.

(iv)That they avoid forming new on-line 'friendships' or enter communication with parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(vi)That they could face legal proceedings if comments they post about named individuals are found to have harmed their reputation.

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 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 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

Staff

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 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:

o Abusive, threatening, harassing and misogynistic messages

o non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

o Sharing of abusive images and pornography, to those who don't want to receive such content

o Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

o develop better awareness to assist in spotting the signs and symptoms of online abuse.

o develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.

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

o The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every year. They will also update their knowledge and skills about 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.

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

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

14. MONITORING ARRANGEMENTS

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

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The Self Review (such as the one available here) will be supported by an annual action plan considering the potential risks. This is important because technology, and the risks and harm 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 policy

Staff disciplinary procedures

Data Protection Policy and Privacy Notices

Complaints procedure

Computing Policy

PSHE Policy

Mobile phone policy

Appendix 1: EYFS and KS1 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:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: ○ I select a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.	

Appendix 2: KS2

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 • 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 which 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 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 3: 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:	
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 relevant staff 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 leads (DSL) 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 do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**