



CEDARS

Short Stay School

Policy Title	Online safety
Written By	Ian Snead
Review Committee	Full
Date Approved	TBA
Review Date	TBA
Responsible for Day to Day Management	Ian Snead



At CEDARS we are committed to ensuring equality of opportunity including providing access and opportunities for all.

Our vision: **“Together we will build a community where relationships, rooted in kindness and care, will change lives.”**

Our purpose is:

- **Restoring Hope**
- **Rebuilding Confidence**
- **Pursuing Potential**

Our values are:

- **Trust**
- **Learn**
- **Grow**

The purpose of this policy statement

CEDARS Short Stay School works with children and families as part of its activities.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices;
- provide staff and volunteers with the overarching principles that guide our approach to online safety;
- ensure that, as an organisation, we operate in line with our values and within the law and statutory guidance in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in CEDARS' activities.

Legal framework This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Summaries of the key legislation and guidance are available on:

- [online abuse](#)
- [bullying](#)
- [child protection.](#)



We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using CEDARS Short Stay School's network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- appointing an online safety coordinator [this may or may not be the same person as your nominated child protection lead]
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate



- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

MAIN POLICY

1. 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 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, fake news, 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 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 (e.g. consensual and non-consensual sharing of



nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

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

2. Legislation and guidance

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

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying:

advice for headteachers and school staff [Relationships and sex 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. This policy complies with our funding agreement and articles of association.

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 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 understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3) Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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 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 ultimately 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) 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

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 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 policy
Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
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 The ICT team

The ICT team is 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. CEDARS are users of the CEOP system and have two allocated CEOP Ambassadors. Their role is 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 regular basis. This includes the use of two systems embedded in CEDARS practice. Firstly, we use the Securus system to monitor our ICT usage. Using this system allows:

- Daily checks on inappropriate use
- A review of internet and PC usage of staff and pupils

The second system is the Test Filtering website. CEDARS have been advised by ESAS to use this online system to ensure our filters are secure. This test is done on a weekly basis by the DSL and ICT team.



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

Ensuring 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. The ICT manager ensures that our filtering and monitoring software operates efficiently. The Deputy Headteacher alongside the CEOP trained staff, are responsible for internet monitoring using CEDARS CEOP systems with technical support from Entrust ICT support. The Headteacher and Deputy Headteacher are responsible for liaising with Entrust ICT support to ensure filtering is effective.

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and 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 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 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 3).

3.8 Teachers using ICT with pupils in lessons or Remote Learning.

The Teacher is responsible for: Ensuring that Online Safety is reinforced to compliment content delivered within the PSHE curriculum. Checking filtering and monitoring systems then logging and reporting (including safeguarding on MyConcern) any concerns to SLT/Safeguarding team.

4. Educating pupils about online safety Online safety is delivered within the PSHE curriculum.

In PSHE, pupils are taught about the benefits and threats to being online and their online identity and wellbeing. Pupils are taught to be responsible and competent users of ICT. Additional content overlaps with the RSE curriculum when appropriate.

All secondary schools have to teach: Relationships and sex education and health education. 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 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 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 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 about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings. The school will let parents 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 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 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. Staff delivering PSHE will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 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

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 the material, or Retain it as evidence (of a possible 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 it's 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 screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people. **

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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

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 AI tools are now widespread and easy to access.

Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. CEDARS 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.

CEDARS will treat any use of AI to bully pupils very seriously, in line with our Behaviour Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and trust, 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 of the internet 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 to 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. 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 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but must hand them to staff to be stored securely on arrival.

Pupils are not permitted to use them during their time in the school day (9am to 3pm). Any allowed use of mobile devices in school time (such as art projects or use in research) by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to: Keeping the device password-protected – strong passwords 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 by 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 3. 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 ICT Manager.

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 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 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.

11. 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:

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

Training will also help staff:

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



- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the Deputy Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual 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.

13. School social media

CEDARS has developed a plan to use social media as a way to engage students, parents and the wider community in regard to our culture, key information, notifications, work and achievements.

The use of social media requires a rigorous overview and detailed plan; along with designated staff to ensure all information shared is monitored, safe and appropriate.

Please see Appendix 3

14. 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



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

Name of pupil:

E-mail and Internet Use Good Practice

Rules for ICT use

The school computer system provides Internet access to students for learning. The E-mail and Internet Use Good Practice statement will help protect students and the school by clearly stating what is acceptable and what is not.

- School computer and Internet use must be appropriate to the student's education.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Memory Sticks or other computer memory systems must not be brought into school unless permission has been given.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the systems must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.



- School filters will pick up any misuse of the system

The LEA may exercise its right by electronic means to monitor the use of the school's computer systems, including laptops, the monitoring of web-sites, the interception of Emails and the deletion of inappropriate materials in circumstances where it believes unauthorized use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorized or unlawful.

Consent Form For Students

Responsible E-Mail and Internet Use

Please complete, sign and return to the school secretary

<i>Pupil:</i>	
<i>Pupil's Agreement</i> I have read and understand the school 'E-mail and Internet Use Good Practice – rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
<i>Signed:</i>	<i>Date:</i>
<i>Parent/Carer's Consent for Internet Access</i> I have read and understood the school 'E-mail and Internet Use Good Practice – Rules for ICT Users' document and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	



<i>Signed:</i>	<i>Date:</i>
<i>Please print name:</i>	
<i>Parent/Carer's Consent for Web Publication of Work, Photographs & Videos</i> I agree that, If selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.	
<i>Signed:</i>	<i>Date:</i>



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:

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)

When online, only age-appropriate materials/websites will be used/accessed.

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 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

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 do so too.

Signed (staff member/governor/volunteer/visitor):

Date:



Appendix 3 (social MEDIA)



Updates could involve the following:



Objectives	Strategy
1. The school's social media will place pupils at the forefront by showcasing student achievements through photos and videos of learning activities.	Utilising photos already taken by staff on a daily basis, the school can share a weekly round-up of highlights. This can link to rewards and celebration assemblies, while also showcasing exceptional work to show parents and carers what pupils are achieving on a day-to-day basis.
2. Sharing the positive environment and learning experiences of the pupils.	"A day in the life" posts can be used to share students' everyday experiences at school. Students may choose to give a short tour or talk about their favourite parts of the school. For those who do not wish to speak on camera, the post could simply follow a student through their day. These features could focus on a specific subject or area of learning to show the structure of lessons and the types of activities pupils take part in. Similar posts could also be used to introduce staff members and the subjects they teach. To highlight the benefits of having a school dog, the school's social media could follow Scout/Ralph around for the day, showing how they supports pupils' wellbeing, engagement, and positive experiences.
3. Increase community engagement	Highlight fundraising and charity events that pupils take part in, sharing updates, photos, and outcomes to celebrate their efforts and raise awareness of the causes being supported. This helps parents, carers, and the wider community see how pupils contribute positively beyond the classroom. Reach out to local businesses and organisations to encourage community connections. By promoting partnerships and collaborative events, the school can strengthen relationships with local employers create engagement between pupils and the wider community.



Considerations

- **Privacy Settings** – should the account be public for community engagement or private to limit access to students, parents and staff.
- **Content Approval** – ensure all posts are approved by staff, follow safeguarding policies. Comments will be monitored to keep interactions safe and appropriate.
- **Consent and Permissions** – Obtain parental and student consent before sharing photos, videos, or personal achievements online.

Aims and Objectives:

The aim is that the school will use social media as a communication tool to keep parents and students informed and connected.

Official school accounts will share updates, important announcements and reminders, as well as news about upcoming events and activities.

Social media will also be used to celebrate students' successes and achievements, highlighting academic and creative accomplishments in a positive and respectful way. Pupils will be encouraged to share their learning and achievements to build confidence and pride.

In addition, the school will use these platforms to promote community engagement by sharing information about school initiatives, partnerships, and opportunities for families and the wider community to get involved.

Target audience:

- **Students** – to share updates, events, achievements in an engaging way.
- **Parents and carers** – to 'bridge the gap' between home and school. Communicate important information, reminders and school news. It will also provide an opportunity to showcase the school's culture, values and successes.
- **The wider community** – including alumni and local organisations to promote engagement and school-community connections.



DRAFT

