Cleeve Meadow School

ONLINE SAFETY AND SOCIAL MEDIA POLICY

Adopted by the Governing Body – May 2023

To be reviewed May 2026

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy applies to all members of Cleeve Meadow school including staff students, volunteers, parents, carers, visitors and community users who have access to and are users of school ICT systems both in and out of the school.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 students' 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.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will where known inform parents/carers or incidents of inappropriate Online safety behaviour that take place outside of school.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head of school 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).

The governor who oversees online safety is David Linsell

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 2)
- Regular meetings with the online safety coordinator/DSL
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering of control logs and reporting to regular governor's meetings.

3.2 The Head of School

The head of School 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/online safety officer

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Lead the online safety group
- Supporting the head of school in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head of school, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs), keeping self-updated with new guidance
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head of school and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Ensuring the school meets online safety technical requirements
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students 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 termly basis
- 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
- Ensures that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed

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

- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy/ Agreement (AUP)
- 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 students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
- Ensuring that they report any suspected misuse or problem to the Head of School/ DSL/ Online safety coordinator for investigation/ action using 'Bromcom/CPOMS'
- Ensuring that opportunities arising within lessons to discuss online safety issues are fully exploited with students embedding online safety issues within all aspects of the curriculum and other activities
- Ensuring that they monitor the use of digital technologies, mobile devices, cameras etc. In lessons and other school activities (where allowed) and implement current policies with regards to these devices
- Ensuring that in lessons where internet use is pre-planned students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Ensuring that digital communications with students, parents' carers are on a professional level and only carried out using official school systems.
- Ensuring online safety issues are embedded in all aspects of the curriculum and other activities
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and in other school activities (where allowed) and implement current policies with regard to these devices

Online safety group

The online safety group are:

DSL, governor for safeguarding and online safety, PHSE lead, school ICT technician

Members of the group will assist the Online Safety Coordinator with:

- Reporting to the governing body
- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision

3.6 Parents

Parents need to understand that their role is crucial in ensuring the need to use the internet/mobile devices in an appropriate way.

Parents are expected to:

- Notify a member of staff or the head of school 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 are also expected to follow guidelines on the appropriate use of:
- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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 students about online safety

Cleeve Meadow School recognises that teenagers and particularly students with SEN can be vulnerable to exploitation through the technologies they use. The school will be highly proactive in addressing these concerns through curriculum time and off timetable events. Students will be taught about online safety as part of the curriculum at both KS3 and 4 and will link with 6th form mentors at Cleeve Park School who will work with the students to develop their understanding of safe use.

In **Key Stage 3**, students 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
- Develop an understanding of how technology can be used to target young people for example for grooming purposes, in order to be alert to inappropriate contact
- Students 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
- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. It will be provided in the following ways:
- A planned online safety curriculum should be provided as part of computing/PHSE/ other lessons and will be regularly revisited through subjects, the wider curriculum and in discussion as it arises.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

- Students are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Sixth form students will also be asked to work with Cleeve Meadow Students to provide peer support and guidance on safe use of the online platforms.

Students will be given the opportunity to apply to become online safety representatives where they can take an active role in guiding safer use working with both older students from Cleeve Park School and younger students at Cleeve Meadow School.

Students, (where appropriate):

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies.

5. Educating parents about online safety

We recognise that parents/carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/ and information about national/local online safety campaigns and literature. Parents will be encouraged to follow guidelines on the appropriate use of:

- The National Online safety platform
- Digital and video images taken at school events
- Access to parents' sections of the website
- Their children's personal devices in the school (where this is allowed)

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head of school.

- Curriculum activities
- Exploiting school events to raise (online) safety messages with the captive audience
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings

- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g
  www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
- Reference to the online prevent platform
  https://www.elearning.prevent.homeoffice.gov.uk/screen3

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 students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and support staff will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, 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 students, 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 students' 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

Any searching of students will be carried out in line with the DFE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All students (where appropriate) 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 and 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 students, 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.

Community Users

Community Users, (therapists, health staff), who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during the school day and they should be kept turned off and out of sight, they are for ensuring safe student travel before and after school but are not required during the school day:

Any use of mobile devices in school by students 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 policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Staff should not use personal electronic devices during the school day except during their breaks and this should be done only when no student is present.

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 the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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 and GDPR.

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).

The DSL and deputy DSL 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.

Governors should take part in online safety training/ awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/ National Governors Association/or other relevant organisation
- Participation in school training/ information sessions for staff or parents

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. 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
- Anti- bullying policy
- Acceptable Use policy

This policy should be read in conjunction with the ‘eSafety Policy for Kemnal Trust Supported Schools’

Appendix 1: acceptable use agreement (students and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • 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 • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • 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, 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 • I agree that the school will monitor the websites I visit. • I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. • I will always use the school's ICT systems and internet responsibly.	
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 students 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 the 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, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • 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 • Share my password with others or log in to the school's network using someone else's details	
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. 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 students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: acceptable use agreement (Community Users)

Acceptable use of the school's ICT systems and the internet: agreement for Community Users	
Name of Community User:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • 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 • Share my password with others or log in to the school's network using someone else's details	
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. 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 students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**