7H: ACCEPTABLE USE AND DIGITAL SAFETY POLICY

Date Reviewed: Autumn Term 2022
Next Review: Autumn Term 2023
Revision number: 13
Reviewed by: BS

1. AIMS

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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- To review the school processes on an annual basis and correct any problems which arise from this audit. These will be managed in a reviewed yearly risk assessment

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying; advice for headteachers and staff
- Relationships and sex education
- Searching, screening and confiscation
- Sexual violence and sexual harassment between children in colleges and schools

It also refers to DfE 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.

3. ROLES AND RESPONSIBILITIES

3.1 THE PROPRIETOR

The proprietor has overall responsibility for monitoring this policy and holding the headteacher to account for its Implementation. The proprietor 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 DSL/Headteacher 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).

3.2 THE HEADTEACHER

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

3.3 THE DESIGNATED SAFEGUARDING LEAD

Details of the school's DSL deputies are set out in our child protection and safeguarding policy as well 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
- 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
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher.

3.4 THE ICT MANAGER (SOFTEGG)

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 monthly 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 anti-bullying policy.

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 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.

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 factsheet - 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).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum. It will be taught through our PSHEE and Computing schemes of work.

From September 2020 all schools will have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety.

KEY STAGE 1

In Key Stage 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

KEY STAGE 2

Pupils in Key Stage 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

BY THE END OF PRIMARY SCHOOL, PUPILS WILL KNOW:

- That people sometimes behave differently online, including by 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 is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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

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.
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 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. Class teachers will discuss cyber-bullying with their class 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 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.
- 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 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 CHILD ON CHILD ABUSE

Child on child abuse is defined as abuse between children. Cameron Vale School will refer to specific guidance in Keeping Children Safe in Education Part five: Child on Child Sexual Violence and Sexual Harassment.

All staff will be aware that child-on-child abuse can occur between pupils of any age and gender, both inside and outside of school, as well as online. All staff will be aware of the indicators of child on child abuse, how to identify it, and how to respond to reports. All staff will also recognise that even if no cases have been reported, this is not an indicator that child on child abuse is not occurring. All staff will speak to the DSL if they have any concerns about child on child abuse.
Child on child abuse can be manifested in many different ways, including:

- Bullying, including cyberbullying and prejudice-based or discriminatory bullying.
- Abuse in intimate personal relationships between peers.
- Physical abuse – this may include an online element which facilitates, threatens and/or encourages physical abuse.
- Sexual violence – this may include an online element which facilitates, threatens and/or encourages sexual violence.
- Sexual harassment, including online sexual harassment, which may be standalone or part of a broader pattern of abuse.
- Causing someone to engage in sexual activity without consent.
- The consensual and non-consensual sharing of nude and semi-nude images and/or videos.
- Upskirting.
- Initiation- and hazing-type violence and rituals, which can include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group, and may also include an online element.

All staff will be clear as to the school's policy and procedures regarding child on child abuse and the role they have to play in preventing it and responding where they believe a child may be at risk from it.
(*Please refer to the Safeguarding and Child Protection Policy*)

6.4 EXAMINING ELECTRONIC DEVICES

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

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

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

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

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 2.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Form time
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school 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

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 3. 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 (*SoftEgg*).

Work devices must be used solely for work activities.

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. 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 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 in an incident report log.

This policy will be reviewed annually by the Headteacher. In the absence of the Headteacher, a member of the SLT will review and update the policy. 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 found in Employment Handbook
- Data protection policy and privacy notices
- Complaints procedure

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:	

At Cameron Vale, we understand the importance and benefits of using computers to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Please could parents or carers read and discuss this agreement with their child and then sign one copy and return to the school office, and keep the other one for reference.

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:
  1. I click on a website by mistake
  2. I receive messages from people I don't know
  3. I find anything that may upset or harm me or my friends

- Use school computers for school work only
- I will 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 prop erly
- 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 permissio n 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 for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 2: KEY STAGE 2 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:	
At Cameron Vale, we understand the importance and benefits of using computers to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times. **Please could parents or carers read and discuss this agreement with their child and then sign one copy and return to the school office, and keep the other one for reference.**	
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:** • I will only use IT in school for school purposes. • I will only use any class e-mail address or any school e-mail address of my own when e-mailing. • I will only open e-mail attachments from people I know, or who my teacher has approved. • I will not tell other people my password. • I will only open my own files. • I will make sure that all IT contact with other children and adults is responsible, polite and sensible. • I will not send anyone material that could be considered threatening, bullying, offensive or illegal. • I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this **I will tell my teacher immediately.** • I will not give out my own details such as my name, phone number or home address. • I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me. • I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe. • I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community. • I know that my use of IT can be checked and that my parent or carer contacted if a member of school staff is concerned about my e-safety. • I will take care of computers/tablets and other equipment • I know that if I break the rules I might not be allowed to use a computer/tablet **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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 3: ACCEPTABLE USE AGREEMENT (STAFF, VOLUNTEERS AND VISITORS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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 applic able), 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 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:**