Online Safety Policy

Carter's Charity Primary School

September 2025

1. **Aims**

Our school aims to:

   a. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
   b. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
   c. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. **Roles and responsibilities**

   a. **The governing board**
      i. The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
      ii. 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).
      iii. The governor who oversees online safety is Mrs Sarah Strahan
      iv. All governors will:
         1. Ensure that they have read and understand this policy
         2. Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

   b. **The headteacher**
      i. The headteacher has oversight alongside the ICT Technician of the school's filtering (Netsweeper) and virus protection (Sophos) systems. These are administered locally and provided through a service level agreement with the local authority who provide our internet connection.
      ii. The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

   c. **The designated safeguarding lead**
      i. Details of the school's designated safeguarding lead (DSL) and back up (DSL) are set out in our child protection and safeguarding policy.
      ii. The DSL takes lead responsibility for online safety in school, in particular:
      iii. Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
      iv. Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
      v. Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

vi. Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
vii. Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
viii. Liaising with other agencies and/or external services if necessary
ix. Providing regular reports on online safety in school to the headteacher and/or governing board
x. This list is not intended to be exhaustive.

4. The ICT Technician (Mr D Stott)

The ICT Technician is responsible for:

a. 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
b. Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
c. Conducting a full security check and monitoring the school's ICT systems on a monthly basis
d. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
e. Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
f. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
g. This list is not intended to be exhaustive.

5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

a. Maintaining an understanding of this policy
b. Implementing this policy consistently
c. Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
d. 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
e. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
f. This list is not intended to be exhaustive.

6. Parents

Parents are expected to:

a. Notify a member of staff or the headteacher of any concerns or queries regarding this policy
b. Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
c. Parents can seek further guidance on keeping children safe online from the following organisations and websites:
d. What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
e. Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
f. Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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).

8. **Educating pupils about online safety**

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

In **Key Stage 1**, pupils will be taught to:

- **a.** Use technology safely and respectfully, keeping personal information private
- **b.** Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

a. Use technology safely, respectfully and responsibly
b. Recognise acceptable and unacceptable behaviour
c. Identify a range of ways to report concerns about content and contact
d. The safe use of social media and the internet will also be covered in other subjects where relevant.

9. **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.

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.

10. **Cyber-bullying**

a. Definition

i. 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.

b. Preventing and addressing cyber-bullying

i. 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.
ii. 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, and the issue will be addressed in assemblies when appropriate.
iii. 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.
iv. 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.
v. 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.

c. Sexting and Child-on-child Abuse

i. The aspects of online safety within this area are dealt with in our specific policies:

1. **Child-on-child** Abuse Policy
2. Behaviour Policy

11. Examining electronic devices

a. Pupils are not allowed to have any electronic device on their person during the school day. 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.

b. 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:

i. Cause harm, and/or
ii. Disrupt teaching,
and/or
iii. Break any of the school rules

c. 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:

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

d. Any searching of pupils will be carried out in line with the DfE's guidance on screening, searching and confiscation.

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

12. 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 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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

13. Staff using work devices outside school

a. 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.

b. 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.

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

14. How the school will respond to issues of misuse

a. 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.

b. 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.

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

15. Training

a. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues and general safeguarding.

b. 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).

c. The DSL and backup 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.

d. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

e. Volunteers will receive appropriate training and updates, if applicable.

f. More information about safeguarding training is set out in our child protection and safeguarding policy.

16. Monitoring arrangements

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

b. This policy will be reviewed annually by the Senior Management Team. At every review, the policy will be shared with the governing body.

17. 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 and our Complaints procedure

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

PUPIL ACCEPTABLE USER AGREEMENT

Parent/Carer Copy – no need to fill & return, please retain for future reference

These rules will keep everyone safe and help us to be fair to others;

- I will only use the school's computers for schoolwork, homework and as directed;
- I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace;
- I will only edit or delete my own files and not view, or change, other people's files without their permission;
- I will keep my logins, IDs and passwords secret and will change them when requested;
- I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies;
- I will only e-mail people I know, or those approved by my teachers;
- The messages I send, or information I upload, will always be polite and sensible;
- I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them;
- I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission;
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me;
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult;
- I am aware that some websites and social networks have age restrictions and I should respect this;
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk;
- I will respect that others need to use the computers. I will log off when I have finished using them and not interfere with their proper operation;
- I agree that the use of computers is monitored for the protection of both others and myself and that my internet usage will be checked from time to time.
- I will not access any information via the internet or store information that promotes radicalisation or extremist behaviours.
- I will not access social media during school hours or on school equipment.
- I will not use a teacher or another student's account and/or falsely set up an account.

I have read and understand these rules and agree to them.

Name (Please PRINT name)	Signed	Class	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 pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: 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 pupils 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**