

Online Safety Policy



Approved by: Claire McGarragh **Date:** 14th November 2023

Last reviewed on: 5th November 2023

Next review due by: November 2024

Contents

1. Rational and aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school.....	9
8. Pupils using mobile and smart technology in school.....	9
9. Staff using work devices outside school.....	9
10. How the school will respond to issues of misuse	9
11. Training.....	9
12. Monitoring arrangements.....	10
13. Links with other policies.....	10
Appendix 1: E-safety agreement (pupils)	11
Appendix 2: acceptable use agreements (taken from the Online Safety and Acceptable Use of IT policy)	11
Appendix 3: online safety training needs – self -audit for staff	12
Appendix 4: online safety incident report log.....	14

1. Rationale and aims

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This online safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put children at risk within and outside the school. 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 semi-nudes and/or pornography), sharing other explicit images and online bullying; and

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

At Cedars Primary School and Nursery, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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.

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

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT Technician and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Paul Wilson.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms of agreement in the Online Safety and Acceptable Use of IT policy (see appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Child Protection 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT Technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT Technician other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (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
- Updating and delivering staff training on online safety (see appendix 3)
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Technician

The IT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly 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 (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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see appendix 2) and ensuring that pupils follow the school's terms on acceptable use (see appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by informing the IT Technician and Designated E-Safety Lead/DSL if they need to bypass the filtering and monitoring systems for educational purposes
- 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's Attitude and 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/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to inform the school if they consent to images of their child being taken and used in the public domain (e.g. on the school's website).
- Agreeing to the Home-School Agreement: Cedars' Live Lessons (where remote learning is necessary)
- Sign a Home Laptop and Ipad Loan-Agreement if a device is required for remote learning

Parents/carers 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 (see [appendix 3](#)).

4. Educating pupils about online safety

At Cedars Primary School and Nursery, pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

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

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

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

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The 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/carers about online safety

The school will raise parents/carers' awareness of internet safety in newsletters, Parent Mail items (weekly 'Wake Up Wednesday' information from National Online Safety), our website and practical training sessions e.g. (Safer Internet Day, NSPCC).

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their child is being taught with regards to online safety

If parents/carers 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.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff will find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school will also make parents/carers aware of the signs of cyber-bullying, 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 's Attitude and 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, 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 of pupils

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

- Poses a risk to staff or pupils, and/or
- Is identified as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher

- Explain to the pupil why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

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

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

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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

- **Not** view the image
- Confiscate the device and report the incident to a DSL 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](#)

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](#)
- The school's Attitude and Behaviour policy

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

6.4 Artificial intelligence (AI)

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

Cedars Primary School and Nursery 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.

Cedars Primary School and Nursery will treat any use of AI to bully pupils in line with our Attitude and Behaviour policy.

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

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see 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 and restrict access through filtering systems where appropriate.

8. Pupils using mobile and smart technology in school

Pupils in key stage 2 may bring mobile phones in to school, but they are not permitted to use them during the school day (this includes extra-curricular activities after school). Parents/carers have to sign a mobile phone agreement and pupils must hand their mobile phone to their class teacher at the beginning of the school day. Their mobile phone will be returned to them at the end of the school day.

Any breach of the agreement will be dealt with according to the school's Attitude and Behaviour policy.

9. Staff using work devices outside school

All staff members will read and sign they agree to the terms in the Online and Acceptable Use of IT policy.

Staff members must not use the device in any way that would violate the school's terms of acceptable use (see appendix 2).

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 IT Technician.

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 Child Protection and Attitude and Behaviour policies. 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 Safer 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 that 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.

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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Children can abuse other children online through:

- Abusive, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

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 the school's Child Protection policy.

12. Monitoring arrangements

The IT Technician and DSLs record safeguarding issues related to online safety in an incident report log (see appendix 4) and in CPOMs.

This policy will be reviewed every year by the Claire McGarragh. At every review, the policy will be shared with the governing board. This is important because technology, and the risks and harms pupils face online evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection
- Attitude and Behaviour Policy
- Online Safety and Acceptable use of IT Policy
- Staff Safer Code of Conduct
- Whistleblowing Policy
- Data Protection Policy and Privacy
- Privacy Notice GDPR Pupils
- Complaints Policy

Appendix 1: E-Safety agreement (pupils)

We use the school computers and internet connection for learning. These rules will help us to be fair to others and keep everyone safe. I will learn and follow the SMART rules.



- ✚ I will ask permission before entering any website unless my teacher has already approved that site.
- ✚ I will keep my personal stuff private and think about what I say and do online.
- ✚ I will learn to block people who send nasty messages and won't open unknown links and attachments.
- ✚ I will flag up any concerns or upsets I have with my teacher.
- ✚ I will only use the programmes and applications that are appropriate for the lesson.
- ✚ I will not interfere with other people's files.
- ✚ I will not bring flash memory sticks into school without permission.
- ✚ I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

I have read the terms of the E-Safety Agreement and I agree to follow them.

Signed

Appendix 2: acceptable use agreements (taken from the Online Safety and Acceptable use of IT policy)

ACCEPTABLE IT USE AGREEMENT

I understand that the school internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the internet and I am aware of the consequences if I breach them.

I am aware that by breaching the rules and regulations it may lead to:

- withdrawal of my user access
- the monitoring of how I use the internet
- disciplinary action
- criminal prosecution

I will report immediately to the IT Technician and Designated E-Safety Lead/DSL any accidental access to inappropriate material or websites that I may have.

I will log on to the Internet by using my password, which will be changed if I think someone knows it.

When using the school's internet I will not:

- use the internet in such a way that it will bring the school into disrepute;
- use inappropriate or illegal websites;
- download inappropriate material or unapproved software;
- disrupt the time of other Internet users by misusing the internet;
- use inappropriate language;
- use language that may provoke hatred against any ethnic, religious or other minority groups;
- produce, send out, exhibit or publish material that will cause offence to anyone;
- divulge any personal information about myself, any other user or that of pupils;
- divulge my login credentials or passwords to anyone;
- use the login credentials or passwords of any other user;
- use a computer that is logged on by another user;
- use any social networking site inappropriately but only to use it in order to develop teaching and learning;
- transfer the images of pupils without prior permission of the Headteacher and from parents;
- use email for private use but only for educational purposes;
- compromise the Data Protection Act (GDPR) or the law of copyright in any way.

ACCEPTABLE MOBILE PHONE USE AGREEMENT

During the school day school personnel are restricted to using their mobile phones to break times and lunchtimes with their mobile phones being switched off during lesson/work times. It is the responsibility of all school personnel to keep their mobile phones securely stored.

- Family members should be informed that in the case of an emergency that staff can be contacted through the school day via the school office;
- Staff are allowed only to use their mobile phones throughout the school day in the case of a personal emergency (this should be discussed with the Headteacher);
- Mobile phones will be switched off or silenced during lesson/work times;
- Mobile phones are to be securely stored;
- Texts messaged should not be sent or received in lessons;
- Camera phones should not be used at any time to photograph a pupil;
- Mobile phones should not be used to send or receive inappropriate texts or images;
- Staff are not to be photographed by a parent or a pupil on a mobile phone;
- Staff are not to give out their mobile telephone number to parents or pupils;
- Staff must use the school telephone to contact a parent and not use their mobile phone;
- Staff must not store parents or pupils telephone numbers on their mobile phones;
- Staff will be issued with a school mobile phone when attending an off-site residential educational visit (this mobile phone is not for private use);
- Staff will not give email address to parents;
- Staff will tell parents that all electronic communications should be via the office.

I agree to abide by the Online and Acceptable Use of IT policy:

Employee Name:		Headteacher Name:	
Employee Signature:		Headteacher Signature:	
Date:		Date:	

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident