

Policy Date:	November 2021	Version: 1.6		
Policy Review Date:	November 2022 November 2023 November 2024 September 2025	Mrs Louise Underwood (Head Teacher)		16.11.2022 25.11.2021 9.11.2024
Adopted by Governing Body:				
Chair Of Governors:		C Brown		19.11.2022 25.11.2021
		E Chester		11.11.2024



Avenue Primary Online Safety Policy 2024 - 2025



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.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 (RSE);
- 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 considers 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 safeguarding governor will co-ordinate regular meetings with appropriate staff to discuss online safety, including online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- ensure that they have read and understand this policy;
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).

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 Online Safety Lead (Deputy 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 Online Safety Lead has 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 technician and other staff, as necessary, to address any online safety issues or incidents;
- ensuring that any online safety incidents are logged (CPOMS) 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 as part of safeguarding training annually (delivered by Leicester City Council);
- as part of induction, new staff will receive training on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. New staff are also given information about monitoring and filtering systems that are in place and sign the code of conduct / acceptable user agreement;
- liaising with other agencies and/or external services if necessary;
- where applicable, updates in regards to online safety are shared in the safeguarding part of SLT meetings and with the governor for safeguarding.

This list is not intended to be exhaustive.

3.4 The ICT manager

(Delegated to the technical support team and other related organisations that have been appointed by the school.)

The technical support team are 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;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- appointed outside agencies will ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of online-bullying are dealt with appropriately in line with the school behaviour policy, including logging on CPOMs.

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, and ensuring that pupils follow the school's terms on acceptable use;
- 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 online-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

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;
- <https://nationalcollege.com/parents>

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.

4. 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:

- 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 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 areas of the curriculum, where relevant. The use of social networking sites is not permitted in school on school equipment.

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. Children will be taught about online safety in line with the national curriculum as well as any current or relevant risks that are apparent in the school community.

As part of RSE curricula, all students will undertake awareness lessons in online safety. This is further reinforced in all other areas of the curriculum, especially when working with technology.

The key messages from these lessons are:

- The dangers of using the internet/apps both at home and at school
- What to do if they come across inappropriate/offensive text or images
- How to stay safe when communicating online
- How to take appropriate action when things go wrong
- How to stay safe when using Social Networking sites such as Instagram, Tik Tok etc.
- How to stay safe in chat rooms/discussion forums
- What to do if they are a victim of cyberbullying
- The dangers and laws of sharing nudes and semi nudes (formally known as 'sexting') as well as sharing inappropriate images/videos

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 or virtual learning environment (VLE). Parents will receive relevant information on the potential dangers of social networking sites, games and apps from the parent guides on the National College and other relevant resources.

This policy will also be shared with parents.

Online safety will be covered during the annual market place events to introduce the year and updates will be emailed out regularly and in response to any concerns.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and/or the phase leader.

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

6. Online-bullying (Or Cyber-bullying)

6.1 Definition

Online-bullying takes place on sites, 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 online-bullying

To help prevent online-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, 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 pupils, as part of safeguarding training.

The school will also send 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 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,
- Retain it as evidence (of a criminal offence or a breach of school discipline),
- Report it to the police,

Examples of illegal activity that may require police intervention would include;

- Child sexual abuse and images (including images of one child held by another child)
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Recordings of criminal activity as a witness (this includes peer on peer abuse, including 'upskirting')
- The use of weapons to injure someone.

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. 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.

8. Personal devices in school

Personal mobile phones and mobile devices

Staff, Parents and Visitors:

- Mobile phones and personal handheld devices brought into school are entirely at the staff members', parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- No images, videos or recordings should be taken on mobile phones or personally owned handheld devices within the school or its grounds without the prior consent of the Headteacher and the person or people concerned.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally owned devices are not permitted in areas of school where children are present, with the exception of DSLs who are on duty.

- Staff may use their phones when not supervising children e.g. during break times as long as no children are present. If a staff member is expecting a personal call (eg. from the GP), the staff member should not answer their phone until they are in a child-free designated area and should request consent from the Headteacher prior to receiving the call. Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times and stored in staff lockers, cupboards or locked desk drawers.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

If, due to unprecedented circumstances, DSL staff are required to use their own phones to contact children, young people or parents, they will do so by withholding their number and with the knowledge of the head teacher.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, the only calls to be made are with the school office, head teacher or emergency services.

- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Pupils may bring mobile devices to school but on arrival they are deposited in the main school office and not collected until the end of the day. Pupil mobile phones are not allowed in the main building only within the reception (main office) area. They are not permitted to use them during:

- the school day or on the school grounds;
- clubs before or after school, or any other activities organised by the school;

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 policy.

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 technical support team.

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 our policies on behaviour policy as well as Acceptable Use 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 policy/ staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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 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 on CPOMs or via report provided by the technical support team. This policy will be reviewed annually by the computing lead and the DSL responsible for online safety. After 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
- ICT and internet acceptable use policy
- RSE policy

14. Responsibilities

Role	Person	Date Responsible
Headteacher	Louise Underwood	09-2024 – 5.1.2025
	Jenny Goddard	6.1.2025 – 31.8.2025
Online Safety Lead (Deputy DSL)	Cathryn Rawlings	01.09.2024- 31.8.2025
Governor	Katie King	01.09.2024- 31.8.2025
IT Manager	MTS	01.09.2024- 31.8.2025

(Technical support team)	(Micro Technology Services) Contact: 0116 4670155	
--------------------------	--	--