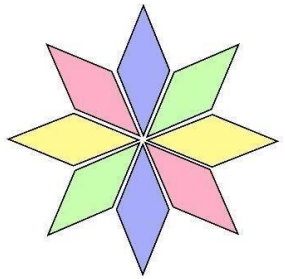

Kaleidoscope School: Online Safety Policy

WE BELIEVE YOU CAN

Date of policy: January 2025
Date of next review: January 2026

Online Safety Policy

The purpose of this policy is to:

- Safeguard pupils through the filtering and monitoring of the use of technology, including mobile and smart technology (which we refer to as 'mobile phones') within school.
- Safeguard pupils by ensuring that they are educated about e-safety issues and appropriate behaviours so that they remain safe and legal online.
- To ensure that as a school we support pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.

Date of policy: January 2025
Date of next review: January 2026

- To ensure that any personal data and information is kept secure.
- To minimise the risks of handling sensitive information.

1. Introduction

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. This policy highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for the users to enable them to control their online experiences.

The School's Online Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole and will operate in conjunctions with other policies including those for Behaviour, Bullying, Curriculum, Data Protection, Child Protection and Safeguarding Policies and ICT agreements.

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

Have robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff and volunteers.

Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones') Set clear guidelines for the use of mobile phones for the whole school community.

Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: child to child 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; for example, 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. If you feel your pupils, pupils or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

To meet our aims and address the risks above, we will:

- Educate pupils about online safety as part of our curriculum. For example:

- *The safe use of social media, the internet and technology*
- *Keeping personal information private*
- *How to recognise unacceptable behaviour online*
- *How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they're a witness rather than a victim.*

- Train staff, as part of their induction on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation, and the expectations, roles and responsibilities around filtering and monitoring. All staff members will receive refresher training as required and at least once each academic year.

- Educate parents/carers about online safety via our website, communications sent directly to them and through parents' events. We will also share clear procedures with them, so they know how to raise concerns about online safety.

- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
  - *Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present.*
  - *Staff will not take pictures or recordings of pupils on their personal phones or cameras.*

- All staff and any visitors using technology must sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology.

- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation

- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems.
  Our filtering and monitoring standards will-

  - identify and assign roles and responsibilities to manage filtering and monitoring systems.
  - review filtering and monitoring provision at least annually.
  - block harmful and inappropriate content without unreasonably impacting teaching and learning.
  - have effective monitoring strategies in place that meet their safeguarding needs

- Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community.

- Provide regular safeguarding and children protection updates including online safety to all staff, at least annually, in order to continue to provide them with the relevant skills and knowledge to safeguard effectively.

- Review the child protection and safeguarding policy, including online safety, annually and ensure the procedures and implementation are updated and reviewed regularly.

Date of policy: January 2025
Date of next review: January 2026

This section summarises our approach to online safety and mobile phone use.

For full details about our school's policies in these areas, please refer to our online safety policy and mobile phone policies.

Guidance Documents:

- Children's Commissioner-Online Safety
- Teaching online safety in education settings
- Appropriate Filtering and Monitoring
- CEOP-Safety Centre
- National Cyber Security Centre
- NSPCC-Undertaking remote teaching safely
- PHSE-Advice on addressing coronavirus (COVID-19)
- 360 Degree Safe - Online Safety Review Tool
- UKCCIS-UK Council for Child Internet Safety

Date of policy: January 2025
Date of next review: January 2026

2. Roles and Responsibilities

Many pupils within Kaleidoscope have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. The professionals occupying the positions below, should endeavour to complete their roles effectively and make themselves familiar with this policy, to ensure our pupils are protected.

The following section outlines the roles and responsibilities of individuals and groups within school.

Headteacher and Senior Leaders

The Headteacher and senior leaders have a duty to ensure that the Designated Safeguarding Lead has suitable CPD to enable them to carry out their roles and to train other colleagues, as relevant.

The Headteacher and senior leaders will ensure that there is a system in place to allow for filtering and monitoring and support those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

Ensure all school mobiles phones, computers and any other device whereby camera usage and/or the internet can be accessed are checked on a 1-2 weekly basis (during term time).

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding and child protection (including online safety),

Keeping Children Safe in Education, 2024. The DSL will meet with a managing director once per term to monitor Safeguarding processes within the school, including Online Safety.

The Designated Safeguarding Lead should be trained in online safety, e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

All other staff

All other teaching staff, or staff whom have direct contact with pupils are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood, and signed the school policy documents
- They report any suspected misuse or problem to the designated safeguarding team.
- Digital communications with pupils should be on a professional level and only carried out using official school systems

- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety policy to the best of their ability.
- They supervise ICT activity/ laptop use for all children.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies about these devices
- If a pupil attempts to access inappropriate material on internet searches this must be reported to the designated safeguarding team immediately.
- Staff must ensure their passwords are secure and refrain from sharing them with anyone else. For reasons of GDPR, staff are advised to change their passwords at least every 6 months.
- Promote online safety and proactively offer support to all families

Date of policy: January 2025
Date of next review: January 2026

3. Curriculum

Why Internet use is important?

The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. **Internet use to enhance learning**

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will use the internet to find and evaluate information to enhance and extend their education. Access to the internet will be a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work. As in other areas of work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the pupils.

- Access to the internet may be by teacher or teaching assistant demonstration.

- Pupils may access teacher-prepared materials, rather than the open internet.
- Pupils may be given a suitable web page or a single website to access.
- Pupils may be provided with lists of relevant and suitable websites which they may access
- More able pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher.

Pupils are regularly reminded of school rules on internet safety and how to be safe online.

Pupils accessing the internet will be always supervised by an adult.

4. Unsuitable / inappropriate / illegal activities

Kaleidoscope believes that the activities referred to in the following section would be inappropriate in our school context and the users (defined below) should not engage in these activities in school our outside when using school equipment. Our school policy restricts certain internet usage as detailed below:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:				
Child sexual abuse images				X
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				X

Adult material that potentially breaches the Obscene Publications Act in the UK				X
Criminally racist material in the UK				X

Date of policy: January 2025
Date of next review: January 2026

Pornography				X
Promotion of any kind of discrimination				X
Promotion of racial or religious hated				X
Threatening behaviour, including promotion of physical violence or mental harm				X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X
Using school systems to run a private business				X
Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school				X

Date of policy: January 2025
Date of next review: January 2026

Uploading, downloading or transmitting commercial				X

software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, completer/network access codes and passwords)				X
Creating or propagating computer viruses or other harmful files				X
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestions and hinders others in their use of the internet				X

Date of policy: January 2025
Date of next review: January 2026

Online gaming (educational)	X			
Online gaming (non-educational)		X		
Online gambling				X
Online shopping			X	
File sharing			X	
Use of social networking sites				X
Use of video broadcasting e.g. YouTube during lesson times with permission		X		

Date of policy: January 2025
Date of next review: January 2026

5. Communications

Communication technologies have the potential to enhance learning. The following table shows how Kaleidoscope currently considers the benefit of using these technologies for education, with their risks/disadvantages in mind.

	Staff				Pupils			
	Allowed	Allowed at certain points	Allowed with permission	Not allowed	Allowed	Allowed at certain points	Allowed with permission	Not allowed

Date of policy: January 2025
Date of next review: January 2026

Mobile phones may be brought into school		X						X

Use of mobile phones in lessons				X Unless a school phone				X
Use of mobile phones in social time		X						X
Taking photos on school camera devices		X					X	

Date of policy: January 2025
Date of next review: January 2026

Taking photos on personal mobile devices				X				X
Use of hand held devices e.g. iPads, PSP's in lessons – educational use	X						X	
Use of personal email addresses in school or on				X				X
School network								
Use of school email for personal emails				X				X

Date of policy: January 2025
Date of next review: January 2026

Use of chat rooms/facilities for personal use				X				X
Use of instant messaging for personal use				X				X
Use of social networking sites for personal use				X				X
Use of blogs			X				X	

6. Use of digital and video images

When using digital images, staff should inform and educate pupils (as appropriate) about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

7. Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

- Transfer data using secure password protected devices.

8. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.;

- Child sexual abuse images

- Adult material which potentially breaches the Obscene Publications Act

- Criminally racist material

- Other criminal conduct, activity, or materials

An ‘urgent’ concern should be raised on school’s safeguarding system, My Concern and this should immediately be reported verbally to the Designated Safeguarding Lead, Amy Sadler-Rhodes or in her absence, to the Deputy Designated

Safeguarding Lead, Sam Goodin. Procedures within Kaleidoscope School Child Protection and Safeguarding Policy and if appropriate, Whistleblowing Policy, should then be followed, and the police informed.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Staff should follow the Kaleidoscope School Child Protection and Safeguarding Policy when reporting incidents impacting on the welfare of pupils and the Whistleblowing policy if appropriate.

Where an incident of misuse is not a Safeguarding or Child Protection concern, staff should refer to the Kaleidoscope School Behaviour Policy as appropriate. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as follows:

- In the case of a Safeguarding or pupil welfare concern, any incident of misuse will be reported immediately to the

Designated Safeguarding Lead or to the Headteacher

- Incidents of Staff/Volunteer misuse (in the case of misuse not impacting on the welfare of pupils) will be reported to the Headteacher and addressed using the Staff Disciplinary Procedures.

Date of policy: January 2025
Date of next review: January 2026

9. Actions and Sanction for Staff

Incidents	Refer to the DSL	Refer to the Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re: filtering	Warning	Suspension	Disciplinary Action

Date of policy: January 2025
Date of next review: January 2026

Deliberately accessing or trying to access material that could be considered inappropriate, against school policy and/ or illegal	X	X	X	X	X	X	X	X

Accessing any content that indicates a risk to the welfare and safeguarding of pupils	X	X	X		X	X	X	X

Date of policy: January 2025
Date of next review: January 2026

Excessive or inappropriate personal use of the internet/ social networking sites/ instant messaging/ personal email	X	X	X		X	X	X	X
Unauthorised downloading or uploading of files		X	X			X	X	X

Date of policy: January 2025
Date of next review: January 2026

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X		

Date of policy: January 2025
Date of next review: January 2026

Deliberate actions to breach data protection or network security rules		X			X	X	X	X

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X	X	X

Date of policy: January 2025
Date of next review: January 2026

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X			X	X	X
Using personal email/social		X				X		

networking/ instant messaging/ text messaging to carry out digital communications with pupils	X	X		X		X	X	X

Date of policy: January 2025
Date of next review: January 2026

Action which could compromise the staff member's professional standing		X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X

Date of policy: January 2025
Date of next review: January 2026

Accessing offensive or pornographic material	X	X	X			X	X	X
Breaching copyright or licensing regulations		X	X			X	X	X
Continued infringements of the above following previous warnings or sanctions		X	X			X	X	X

Date of policy: January 2025
Date of next review: January 2026

10. Training

All new staff members will receive online safety training, as part of their induction.

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

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
- Children can abuse their peers 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

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 designated safeguarding team 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.

Volunteers will receive appropriate training and updates, if applicable.

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

11. Policy review

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the proprietors. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Date of policy: January 2025
Date of next review: January 2026