Micklands Primary School

Online Safety Policy

Publication date: 1st September 2024

Review date: 31st August 2027

Status: Non-statutory

Contents:

1. Introduction

Micklands is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers and governors. We use training, education and effective procedures to both educate and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.
In line with Keeping Children Safe in Education, we aim to address the following 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: 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; 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.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

2. Roles and responsibilities

2.1 The governing body:

- Take overall responsibility for this policy and its implementation.
- Read, and understand this policy.
- Ensure the policy is reviewed and updated.
- Ensure students are taught about online safety.
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated.
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures.
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

2.2. Headteacher:

- Ensure staff understand this policy.
- Ensure the implementation of this policy is consistent across the school.
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter.
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns.
- Ensure appropriate filtering and monitoring systems are put in place.
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online.
- Ensure that the school's ICT systems are secure and protected against viruses and malware.
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received.

2.3 Designated Safeguarding Lead:

- Support the headteacher in implementing this policy.
- Oversee the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead.
- Work with IT technicians, computing lead and staff to address any online safety concerns or incidents, in line with the Child Protection and Safeguarding Policy.
- Liaise with external safeguarding partners as necessary, including children's social care and the police, and make referrals with the support of relevant colleagues and their expertise.
- Ensure any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents.
- Deliver staff training on online safety.
- Provide regular updates regarding online safety incidents to the headteacher.
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received.
- Ensure that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

2.4 All staff and volunteers:

- Read and understand this policy.
- Assist with the consistent implementation of this policy.
- Agree with and follow the Acceptable Use of ICT agreement.
- Agree with and follow the Staff Code of Conduct, which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Refer any online safety safeguarding concerns to the DSL or a Deputy DSL through CPOMS.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.

- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.

2.5 Parents:

- Understand the importance of children being safe online.
- Read, understand and comply with this policy.
- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access, and who from the school (if anyone) will be interacting with their child.
- Notify a member of staff regarding any questions regarding this policy and its implementation.
- Support their child to behave safely and appropriately online.

3. Teaching online safety

In line with 'Teaching online safety in school,' published by the Department for Education in June 2019, we teach pupils about online safety and harms. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These skills are covered in Computing and PSHE.
Throughout this, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online.
- the risks posed by social media platforms.
- how to recognise techniques used for persuasion.
- unacceptable online behaviour.
- how to identify online risks.
- how and when to seek support.
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online.
- how elements of online activity can adversely affect a pupil's wellbeing.

We recognise that there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We will ensure these pupils receive the information and support they need through our pastoral support.

In addition, our school completes an annual risk assessment for online safety. We consider the updated non-statutory guidance (Jan 2023) from the DfE on teaching online safety and how we teach these elements.

4. Filtering and monitoring

Micklands uses RM SafetyNet as a filtering and monitoring system. This filters and monitors for pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, harmful online interaction with other users, personal online behaviour that increases the likelihood of, or causes, harm and risks such as online gambling, inappropriate advertising, phishing and or financial scams. This covers all devices that connect to our school network.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies monitor the effectiveness of this system through analysing the weekly report on the terms and sites being accessed or attempted to be accessed on the network. They also regularly check that the filtering is appropriate by attempting to access certain sites.

The school takes care to not over block content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

The DfE has published filtering and monitoring standards which set out that schools should:

- 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 reasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

We at Micklands have done the following in relation to this:

- Assigned the DSL to be responsible for the overall management of the filtering and monitoring systems.
- Reviewed the filtering and monitoring systems at least annually and at Safeguarding Team meetings.
- Ensured that search restrictions are robust and harmful content blocked.
- Monitored search terms and websites accessed, or attempted to access, weekly.
- Analysed and looked for patterns in blocked searches and/or sites.
- Communicated concerns to teachers and worked with them to adapt lessons and/or the curriculum as required.
- Ensured that all concerns are logged.
- Communicated any concerns to parents.

When the filtering and monitoring system detects concerning usage, we will record this on CPOMS and take appropriate action, including a referral to children's social care when necessary.

5. Security

Micklands has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies.

6. Educating parents about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety, we provide regular updates in the school newsletter and other communications. We also share our computing and PSHE curriculums with parents.

7. Acceptable Use agreement

All 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. Any breaches of this agreement can lead to disciplinary procedures.

8. Use of mobile and smart technology

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). Children in Year 5 and 6 are permitted to bring a phone to school, but this must be turned off once on site and handed in to their class teacher. It should not be turned back on until they have left the school site. However, outside of school, this access means some children can sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To manage this and reduce risk, we educate our children about the safe use of the internet and mobile devices in our Computing and PSHE curriculums. We also regularly keep parents updated with the risks and ways to protect their children through the newsletter and other communications.

Our Staff Code of Conduct outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

9. Training and staff knowledge

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. This will also include training on the filtering and monitoring system used by the school and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as relevant updates (for example through emails and staff meetings).

The DSL and Deputy DSLs 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 about online safety at regular intervals, and at least annually.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.
- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online, this can take the form of:
    - Online abuse, including sexual.
    - Online harassment, including sexual.
    - Cyberbullying.
    - Misogynistic / misandrist messages.
    - The non-consensual sharing of incident images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.

- That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

10. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarded. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals to, or seeking advice from, Children's Social Care, our local Prevent team and/or the police.

For **parents** the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- Thinkuknow - how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For **students** the following websites could be of use:

- Mind - mental health support
- Togetherall - online community accessible 24/7
- Shout - a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For **all staff and volunteers** it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- UK Safer Internet Safety - teacher guides and resources
- https://www.internetmatters.org/schools-esafety/
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Policies / guidance to be read and understood alongside our Online Safety Policy:

- Child Protection and Safeguarding Policy.
- Behaviour Policy.
- Staff Code of Conduct.
- Acceptable Use of ICT Policy and Agreement.
- Anti-Bullying Policy.
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology standards in schools and colleges (DfE)

Appendix 1 – Online Safety Risk Assessment

	Statement	Evidence	RAG Rating	Action required
Policy	There is a policy covering online safety at the school			
	Staff have been made aware of this policy			
	This policy has been reviewed and updated this academic year			
	Remote learning is covered in this policy			
	The school has a clear policy on pupils' personal devices, including mobile phones			
Staff training	Staff and governors have been trained in online safety this academic year			
	Online safety, including filtering and monitoring, is covered in staff and governor inductions			
Curriculum	Pupils have been taught about online safety* ** For an in-depth analysis of this see Appendix A*			
	Pupils' knowledge of online safety has been tested			

	Statement	Evidence	RAG Rating	Action required
	Pupils with SEND are supported to learn how to stay safe online			
	Pupil feedback is sought on the online safety curriculum			
Parental engagement	Our school engages parents in our commitment to online safety			
	Parents are updated around what their children are being asked to do online			
Filtering and monitoring systems	Our school has a filtering and monitoring system in place			
	The provider of this system is signed up to relevant lists detailed in KCSIE (*KCSIE 22, para 142 – you can test this here*)			
	The school has reviewed the DfE published filtering and monitoring standards and are compliant with this.			
	The DSL knows that they have lead responsibility for this area			

	Statement	Evidence	RAG Rating	Action required
	This system is regularly reviewed at least annually. Leaders make care not to unreasonably impact teaching and learning by over blocking content.			
	This system is installed on all devices issued by the school.			
	Staff have received training on filtering and monitoring so that they understand the provision in place, how to manage it effectively, and know how to escalate concerns.			
	Monitoring alerts of inappropriate conduct are sent to relevant members of staff, including the DSL.			
	Alerts of concern are addressed.			
	Alerts of concern are recorded on our record keeping system.			
Cyber security	We have appropriate cyber-security in place to safeguard our IT systems.			

	Statement	Evidence	RAG Rating	Action required
	This security is periodically reviewed.			
Specific incidents	We have addressed a concern about online safety this academic year.			
	We have prepared an anonymised case study on this incident to highlight what went well and what could have gone better.			
	We analyse for trends on our reporting system and respond proactively to reduce online risks and improve online safety.			
Governors	The schools child protection policy and online safety policy are compliant with statutory and best-practice guidance and fit for purpose.			
	The governing body knows that all staff have undergone safeguarding and child protection training which includes online safety at induction. This training is regularly updated.			

Statement		Evidence	RAG Rating	Action required
	The governing body ensures that online safety is a running and interrelated theme when devising the whole-school approach to safeguarding.			
	Governors have oversight of this document and are aware of where actions need to take place to improve practice.			

Appendix 2 – Curriculum Risk Assessment

Underpinning Knowledge and behaviours				
	Content	Y/N	When/ Where e.g., year group, what subject/ lesson	Action Required
Are pupils taught to consider how to evaluate what they see online:	whether a website, URL or email is fake			
	what cookies do and what information they are sharing			
	if a person or organisation is who they say they are			
	why a person wants them to see, send or believe something			
	why a person wants their personal information			
	the reason why something has been posted			
	whether something they see online is fact or opinion			
Are pupils taught to recognise techniques used for persuasion:	online content which tries to make people believe something false is true or mislead (misinformation and disinformation)			
	techniques that a company(ies) might use to persuade people to buy something			
	ways in which criminals may try to defraud people online			
	ways in which games and social media companies try to keep users online longer (persuasive or sticky design)			
	grooming and manipulation techniques used by criminals.			
	ways to protect themselves from a range of cyber crimes			
Are pupils taught in regard to online behaviour:	that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others			
	to recognise unacceptable behaviour in others			
Can pupils recognise acceptable and unacceptabl	looking at why people behave differently online, for example how anonymity and invisibility affect what people do			
	considering unacceptable online behaviours often passed off as 'banter'			

	looking at how online emotions can be intensified resulting in mob mentality			
	looking at the key principles behind a constructive discussion, including a willingness to listen to other opinions and a readiness to be educated on a topic			
	considering how to demonstrate empathy towards others			
	teaching techniques to defuse or calm arguments and disengage in unwanted contact			
Are pupils taught to identify and manage online risk by discussing:	the ways in which someone may put themselves at risk online.			
	risks posed by another person's online behaviour.			
	when risk taking can be positive and negative			
	online reputation and the positive and negative aspects of an online digital footprint			
	sharing information online and how to make a judgement about when and how to share and who to share with			
	the risks of cybercrime, online fraud, and identity theft			
Are Pupils aware of how and when to seek support:	identification of trusted adults			
	access internal support in school e.g., DSL or other relevant staff member			
	Do Pupils know how to access the CEOP service, or Childline			
	Report cybercrime through Action Fraud or the Advertising Standards Authority			
	through reporting inappropriate content or contact for various platforms and apps			
Do Pupils under stand the 5 ...:	The risks of sharing personal data and how to protect their privacy			
	How the online environment operates			

	How online content is generated and to critically analyse the content they consume			
	That online actions can have offline consequences, and use this understanding in their online interactions			
	How to participate positively in online engagement, while understanding the risks of engaging with others			
Teaching about harms and risks				
Age restrictions	Pupils know that age verifications exist, and some sites would require them			
	Pupils understand how this content can be damaging to under-age consumer			
	Pupils know the age of digital consent (13) and that this is the age that young people can agree to share information and sign up to social media without parental consent under GDPR			
How content can be used and shared	Pupils know what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications			
	Pupils know how cookies work			
	Pupils know how content can be shared, tagged and traced and how difficult it is to remove something a user wish had not been shared			
	Pupils know the risk of identity theft or targeted approach from fraudsters using information shared online			
	Pupils know what content online is illegal including: • youth-produced sexual imagery • sharing illegal content such as extreme pornography or terrorist content • the illegality of possession, creating or sharing any explicit images of a child even if created by a child			
Teaching on disinformation, misinformation	Pupils know what disinformation is and why individuals or groups choose to share false information to deliberately deceive			
	Misinformation and being aware that false and misleading			

	information can be shared inadvertently			
	Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs (including revenge porn)			
	Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons.			
	Explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online.			
	How to measure and check authenticity online			
	the potential consequences of sharing information that may not be true.			
Veracity of information	Pupils are taught about fake websites and scam emails which can be used to extort data, money, images and other things			
	Pupils know what fake URLs/ websites look like, the risks of entering websites that are not secure, and the risk of 'too good to be true offer'			
	Pupils know what to do if harmed, targeted, or groomed as a result of a fake website or scam email and know how to access support			
	Pupils are aware of identity fraud and the risks of scams and phishing and that this can be highly sophisticated			
	Pupils know how to identify what good companies will and won't do when it comes to personal details, and by consequence what criminals might do			
	Pupils know how to report fraud, phishing attempts, suspicious websites and adverts			
Protecting personal information	Pupils know why passwords are important and how to keep them safe			
	Pupils know how to identify phishing scams and the importance of online			

	security to protect against viruses that can take password			
	Pupils are aware of how their data is farmed and why. They know how to protect themselves			
	Pupils know of their rights under the General Data Protection Regulations and how to limit the data companies can gather			
	Pupils know about privacy settings including their importance and limitations			
Persuasive design and social media	Pupils know the techniques that companies will use to keep users online for longer			
	Pupils know how adverts seen at the top of online searches and feeds have come from paying companies and that different people see different adverts			
	Pupils know how this targeting occurs and the concept of clickbait			
	Pupils know of the risk of seeing extreme or radical content through this			
How to stay safe online				
Online abuse	Pupils know about the types of online abuse including sexual, harassment, bullying, trolling and intimidation			
	Pupils know when this can become illegal, such as forms of hate crime and blackmail. They know how to report concerns, including ones from anonymous sources			
	Pupils understand the impact of this behaviour on victims and know how to behave appropriately online			
Online Radicalisation	Pupils know how to recognise extremist behaviour and content online			
	Pupils understand actions which could be identified as criminal activity and know how to access support			
	Pupils understand the risks of radicalisation online and how organisations will use social media to identify and target individuals			

Online Challenges	Pupils know what online challenges are and how some can be dangerous or even illegal			
	Pupils know how to assess the risk of an online challenge and where to go for help if they are worried			
	Pupils particularly understand the importance of telling an adult about challenges which include threat or secrecy			
Content which incites	Pupils know that online content can glamorise the possession of weapons and drugs			
	Pupils know that to intentionally encourage or assist an offence is also a criminal offence			
	Pupils know how to get support			
Fake profiles and online grooming	Pupils know that people may pose as someone they are not online or may be bots.			
	Pupils know how to look out for fake profiles e.g., profile pictures that do not look right, accounts with no followers or thousands of followers, a public figure without a verified account			
	Pupils have an understanding of grooming, and that people can be groomed for radicalisation, sexual abuse and exploitation, gangs and county lines and financial exploitation			
	Pupils know the key indicators of grooming behaviour			
	Pupils know what to do if they are concerned about this behaviour			
Student online activity	Pupils know the risk of live streaming and the potential for people to record this and share the content without the user's knowledge			
	Pupils understand the risk of watching videos that have been livestreamed			
	Pupils understand the importance of not feeling pressured into online behaviour they are not comfortable with			
	Pupils understand that grooming can occur through this medium			

	Pupils should know that pornography is not an accurate portrayal of adult sexual relationships			
	Pupils should know that viewing pornography can lead to a distorted picture of sexual relationships, including normalising violent sexual behaviour			
	Pupils know what revenge porn is and the risks that people have been trafficked into sex work			
	Pupils know that unsafe communication exists online and that consent matters			
	Pupils know to keep their personal information private and know how to say 'no' to both friends and strangers online			
	Pupils know about image filters, the role of social media influencers, and that 'easy money' lifestyles could be too good to be true			
	Pupils know that online behaviour can be an exaggerated picture of people's lives			
	Pupils understand the need to evaluate critically what they do online, including: • screen time length • quality interaction versus quantity • enjoyment versus habit • balanced lifestyle • impact of social media on mental health • where to get help			
	Pupils understand that topics such as eating disorders, self-harm and suicide could be content that they see online. Pupils know how to seek support for this.			
Resources				
Vulnerable students	The school ensures that the curriculum is tailored to meet the needs of SEND and LAC students who may be more vulnerable online			

External sources and visitors	Where the school decides to use external resources and/ or visitors they have vetted for: • where the organisation gets the information from • the evidence base • quality assurance process • background of organisation • whether resources are age-appropriate			
Culture				
Safeguarding	The school creates a safe environment for students to say what they feel and report concerns			
	The school considers that some students could have experienced harmful behaviour online and are sensitive to this when delivering the curriculum			
	The school considers who may be especially impacted by lessons and carefully plans for this			
	Pupils are clear on reporting mechanisms as lessons may prompt students to come forward			
	Pupils are taken seriously when the report concerns and action reinforces the lessons they have received			
	Students and parents have supported the development of materials			
	Schools work with parents to ensure they can support their child to stay safe online at home			
	The school community is aware of the filtering and monitoring processes in place and their role in relation to this.			