Online Safety Policy

Approved October 2025
Review due by September 2026

Contents

Introduction

At Kingsbury Primary School, we recognise the importance of online safety in ensuring the well-being of our pupils. This policy outlines our approach to protecting children from online risks while providing a safe digital learning environment tailored to their needs.

Aims

- To safeguard pupils from online risks including harmful content, inappropriate contact, and commercial exploitation (the 4 C's).
- To implement robust filtering and monitoring systems.
- To educate pupils, staff, and monitoring systems.
- To provide a safe and supportive digital learning experience for all pupils.

The 4 C's of Online Safety
We adopt a structured approach based on the four key areas of online risk:

***Content**: Ensuring children are protected from harmful, misleading, or inappropriate content.*
- Implementing age-appropriate filtering to block harmful material.
- Teaching pupils where appropriate how to recognise and report inappropriate content.

***Contact:** Preventing pupils from being exposed to online predators or harmful interactions*
- Monitoring online communication within the school network.
- Educating pupils, parents and carers about safe interactions and who to report concerns to.

***Conduct**: Encouraging responsible and respectful online behaviour.*
- Teaching digital etiquette and the impact of online actions.
- Encouraging pupils to think before they post or share content.

***Commerce:** Protecting children from fraud, scams, and inappropriate advertising.*
- Blocking online advertisements and commercial content where possible.
- Teaching pupils where appropriate about recognising scams and misleading offers.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Roles and Responsibilities

The Governing Body

The governing body will be responsible for oversight and accountability:

Ensuring that this policy is effective and complies with relevant laws and statutory guidance including DfE's 'Filtering and Monitoring Standards for Schools and Colleges.'

Reviewing this policy on an annual basis and more frequently as and when required.

Ensuring their own knowledge of online safety issues is up to date by participating in regular online safety training (suggested via platforms like BlueSky/ The National College).

Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with and service providers, whilst avoiding "over-blocking" that could restrict educational content or safeguarding teaching.

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.

The Headteacher

The Headteacher will be responsible for operational oversight:

To provide support to the DSL in implementing the online safety strategy.

Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

Conduct risk assessments with the DSL and School Business Manager before making changes to the monitoring and filtering systems.

Manage concerns about staff online behaviour.

Working with the DSL, School Business Manager, and Governing Board to update this policy on an annual basis.

The Designated Safeguarding Lead

The DSL will be responsible for strategic leadership:

Taking the lead responsibility for online safety in the school.

Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.

Lead staff training on online safety, including signs of grooming, exploitation, and

mental health impacts at regular intervals and at induction.

Liaising with relevant members of staff on online safety matters, e.g. the ICT Lead and RSHE lead.

Ensuring online safety practices are audited and evaluated.

Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

Concerns regarding online safety breaches and inappropriate internet use, both by any member of staff or the wider school community using the school's complaints procedure.

Understanding the filtering and monitoring processes in place at the school.

Maintaining and understanding the purpose of detailed, secure, and accurate records of reported online safety concerns, as well as the decisions and whether referrals have been made.

Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.

Working with the Headteacher, School Business Manager and Governing Board to update this policy on an annual basis.

Liaising with external agencies (e.g. police, children's social care) when necessary.

ICT Third-Party

Blue Orange (ICT third-party) will be responsible for:

Providing technical support in the development and implementation of the school's online safety policies and procedures.

Implementing appropriate security measures as directed by the School Leadership Team.

Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All Staff

All staff members will be responsible for day-to-day implementation:

Must be aware and know the signs of online risks including grooming, cyberbullying, radicalisation, and harmful sexual behaviour through regular training delivered by the DSL.

Handle disclosures in line with the Child Protection and Safeguarding Policy.

Deliver online safety education across the curriculum (particularly in PSHE, RHSE, and Computing or Technology).

Supervise pupils using technology and ensure resources are age-appropriate and safe.

Report concerns about online behaviour, hoaxes, or harmful challenges to the DSL.

Follow the Acceptable Use Agreement, staff code of conduct, and maintain a professional level of conduct in their personal use of technology.

Participate in online safety training and stay updated via email communications.

Ensure photographic consent is respected and sensitive data is protected.

Taking responsibility for the security of ICT systems and electronic data, they use or have access to.

To ensure passwords are compliant with security measures, are not shared with anyone else, and that devices are not left unprotected.

Pupils

Pupils (where appropriate) will be responsible for:

Adhering to the Acceptable Use Agreement and other relevant policies.

Seeking help from school staff if they are concerned about something they or a peer have experienced online.

Reporting online safety incidents and concerns to the Teacher who will then be responsible for making reports to the DSL.

Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training through The National College.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Parents are given updates on our approach to online safety, and any training we are facilitating through information on the school website / social media / parental communications and a monthly online safety newsletter.
- Online safety is an agenda item at the DSL meeting.

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. Following our Safeguarding policy, the DSL will consider whether or not this is appropriate or safe, but confidentiality will not be promised. If appropriate, the DSL will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child, and how the report will progress. Information may be shared lawfully under UK GDPR if it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled carefully. The reasons for sharing the information should be explained to the victim and appropriate, specialised support should be offered.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members (e.g. the Headteacher, School Business Manager, Blue Orange) and manages concerns in accordance with relevant policies depending on their nature, e.g. Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and because of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will manage such cases in line with the Child Protection and Safeguarding Policy. All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Antibullying Policy. Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.

- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook.
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse.
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry. The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND (all pupils at Kingsbury).

Child-on-Child Sexual Abuse and Harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is

created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child Sexual Exploitation (CSE) and Child Criminal Exploitation

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age/developmental range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully. In addition, the school will implement a cyber awareness plan for pupils (where appropriate) and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber-crime.

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Risk Assessments.

Online Safety Training for Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. Staff training will also include responsible use of AI, our AI policy, and how to keep the children safe with AI.

All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online Safety and the Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages. School use resources from the NSPCC Techosaururs Scheme

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- Knowledge and behaviours that are covered in the government's online media literacy strategy.

The online risks pupils may face online are always considered when developing the curriculum.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need, in a way that they can understand e.g. simplified language/visuals.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers.
- Laptops.
- iPads.
- Interactive Whiteboards.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

There are appropriate posters in classrooms which are regularly reviewed with the children to support their online safety awareness at an appropriate level.

Use of Smart Technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices.

Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils. The school is committed to ongoing online safety support for parents and carers to educate adults in how to keep their child safe online.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Regulation/Behaviour & Relationships Policy.

The school deliver lessons, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. The ICT lead, RHSE lead and DSL will run a parenting online safety session annually and update the website / newsletter with appropriate resources for parents to access. We also employ a third-party company (Knowsley City Learning Centres) to provide a termly online-safety briefing to parents alongside a monthly newsletter which is distributed via email, our school newsletter, and our website.In addition staff receive a termly online safety briefing to ensure they are aware of any new threats to online safety.

Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child (where appropriate) to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Newsletters.

- Online resources including access to training.
- Online Safety Drop-In Service (parents can bring their children's iPads and tablets for us to help ensure they are safe online).

Internet Access

Staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement, which is kept in the School Business Manager's Office.

Pupils will be made aware of the Online Safety Rules displayed in every class.

Visitors to school will only have access to Wi-Fi through a visitors log-in which has restricted access.

Staff must not access the school internet on personal devices. Staff devices must be in their bag in the cupboard and used only during break times away from children. Refer to staff handbook for more details.

Filtering and Monitoring Online Activity

The Governing Board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges. The Governing Board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems the school implements will be appropriate to pupil's ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The DSL and school business manager will undertake half-termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Prior to making any changes to the filtering system, the Headteacher and DSL will conduct a risk assessment. Any changes made to the system will be recorded. Reports of inappropriate websites or materials will be made to the Headteacher or DSL who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the Headteacher and DSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Regulation/Behaviour & Relationships Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Photographs of children shared with other families or online

When a child starts at Kingsbury Primary School their parents/carers are asked to complete photographic sharing consents. Parents/Carers have the right to change permissions at any time. It is the responsibility of the class teacher to check photographic consents for the children in their class, and to ensure that they adhere to parent/carer wishes. It is important that photographs do not have names on them, including in the background such as names on pictures, labels on wheelchairs, posters, or information in the background. When a child cannot be in a group image it is preferable to blur their face rather than use an emoji over it so that attention is not drawn to them.

Network Security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by our third party ICT provider. Firewalls will be switched on at all times.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the School Business Manager.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils, where appropriate, will use their own unique username and private passwords, which are kept by their class teacher. Staff members will be responsible for keeping their passwords private. Passwords will have a minimum of 6 characters and maximum length of 12 characters and require a mixture of letters, numbers, and symbols to ensure they are as secure as possible.

Users will inform the School Business Manager if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, and Acceptable Use Agreement.

Staff (including long-term supply staff) will be given approved school email accounts. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail and report the matter to the School Business Manager. The school's monitoring system can detect inappropriate links,

malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative Artificial Intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age/developmental stage.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

Staff should use generative AI in accordance with our AI policy, only using approved AI programmes, and never inputting any sensitive, personal, or pupil data.

Social Networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

The School Website

The Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date, and meets government requirements.

Use of Devices

Staff members and pupils may be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the School's Acceptable Use Policy.

The use of personal devices on the school premises and for the purposes of school work from home will be managed in line with Acceptable Use Policy.

Monitoring and Review

The school recognises that the online world is constantly changing; therefore the DSL, school Business Manager, and the Headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness. The governing board, Headteacher, online safety team, and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is October 2026.

Any changes made to this policy are communicated to all members of the school community.

Contributors

Ruth Watkinson
Helen Smith
Rebecca Cunliffe
Katie Gordon-Morris
Becky Benson

All teachers have been consulted March 2025. Updated October 2025