



Kings Mill School & Residence

Online Safety Policy

Approved by: Full Governing Body 18th June 2026

Last reviewed: June 2026

Next review: Autumn 2027

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. The curriculum
4. Staff training
5. Educating parents
6. Classroom use
7. Internet access
8. Filtering and monitoring online activity
9. Network security
10. Emails
11. Social networking
12. The school website
13. Use of school-owned devices
14. Use of personal devices
15. Managing reports of online safety incidents
16. Responding to specific online safety concerns
17. Remote learning
18. Monitoring and review

Appendices

Appendix 1 – Online harms and risks – curriculum coverage

Statement of intent

Kings Mill School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are several controls in place to ensure the safety of pupils and staff.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. 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.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE (current) 'Keeping children safe in education'
- DfE 'Teaching online safety in school'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children & young people.'

This policy operates in conjunction with the following school policies:

- Countering-bullying Policy
- Acceptable Use Policy
- Data and E-security Breach Prevention and Management
- Child Protection and Safeguarding Policy
- Relationships and Sex Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy
- Data Protection Policy
- Photography & Images Policy
- Remote Education Policy
- Use of internet policy and guidelines
- Mobile Devices Policy
- Communication Policy

Roles and responsibilities

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead (DSL) remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training including online safety at induction and regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with IT service providers.
- Ensuring that school leaders and 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.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The Headteacher is responsible for:

- 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.
- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- 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.
- Liaising with relevant members of staff on online safety matters, e.g. the ICT Co-ordinator and the ELSA's
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring 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.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- 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 head teacher and ICT Co-ordinator to update this policy on an annual basis.

The Senior Leadership team are responsible for:

- Providing regular short training updates to staff on any new threats to young people's safety in terms of social media and gaming platforms.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Monitor the effectiveness of the filter and monitoring systems and escalate concerns if necessary.

The ICT Co-ordinator and School Business manager are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and ensuring that all staff have the knowledge and capability to carry out the school reporting procedure.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

- Liaising with the DSL to audit online safety practices and make changes where needed.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

The ELSAs are responsible for:

- Providing support to pupils who are having issues with online safety.
- Work with ICT Co-ordinator to create resources which can be used within the curriculum.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours and ensuring the environment offers prompts and reminders about online safety.
- Maintaining a professional level of conduct in their personal use of technology.
- Ensuring they are the only person using their individual staff log-in (in order to safeguard pupils and to be able to identify who may have been exposed to harmful content.)
- Having an awareness of online safety issues and attended regular short training sessions on online threats.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Ensuring that technology can be used effectively as part of the curriculum. Where filters block sites that are needed for learning, teachers will report this so that the DSL can ensure progress is not affected and ways forward are agreed.
- Supervising children effectively during the use of technology and reminding pupils of safe online behaviours throughout.
- Ensuring that all online communications with parents or carers (via email, ClassDojo) are professional, positive and effective.

Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Online safety and the curriculum

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

- Relationships and Sex Education
- Health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

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
- Who to alert if they feel at risk

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.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk; content, contact, conduct and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The school recognises that, while any pupil can be vulnerable online, our pupils may be more susceptible to online harm or have less support from family and friends in staying safe online.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL 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 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are 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 ensures a safe environment is maintained in which pupils feel comfortable to say what they feel 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 schools reporting procedures around filtering and monitoring.

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.

Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

All staff that are involved in ICT with the pupils will receive training including how the internet can facilitate abuse, staff also receive regular online safety updates as required and at least annually.

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. 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.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Key staff members in the school (DSL, ICT Staff and ELSA Staff), will receive specific E-Safety Training.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role; this includes online safety training. This training is updated at least every two years. However, where external factors such as new apps e.g. pupils in the school are on a new app which is causing them some level of threat.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.
- All staff receive a copy of this policy and should read it and confirm they understand the guidance. New staff will be signposted to a copy of this policy upon their induction. Staff will be informed of any changes to the policy.
- Staff are required to always adhere to the Staff Code of Conduct, which includes provisions for the acceptable use of technologies and the use of social media.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

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 is raised in the following ways:

- Via the school website, online safety page
- Reminders through the school website and ClassDojo app

If a pupil breaches any internet safety guidelines or is exposed to any material considered to be harmful, parents will be informed the same day. They will then be supported to continue offering consistent advice and guidance at home.

Support is available for parents who are worried or concerned about their child's use of technology. The Home School Liaison Officer, DSL or ICT coordinator will refer parents to appropriate internal or external support services.

Use of technology in the Classroom use

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

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras
- Interactive screens
- Smart phones – only after a risk assessment has been carried out and where an individual is judged to require the use of a mobile device for educational purposes.
(See mobile devices policy)

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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

iPads are to be 'locked down' to prevent pupils accessing inappropriate websites and / or downloading apps without the teacher's permission. Class teachers will have the ability to unlock websites and / or the Appstore to unlock websites / apps required for lessons.

Internet access

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement Policy.

All members of the school community are encouraged to use the school's internet network for class-based activities, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The East Riding of Yorkshire Council ensures the school's ICT network has appropriate filters and monitoring systems in place. This is powered by Smoothwall.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system are directed to the DSL or School Business Manager, who will liaise with our Local Authority ICT service.

Prior to making any changes to the filtering system, ICT technician and the DSL will conduct a risk assessment. Any changes made to the system are recorded. Reports of inappropriate websites or materials are made to the DSL and School Business Manager immediately, who investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and School Business Manager, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Positive Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy.

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 are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding policy.

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the School Business Manager alongside our third-party IT support partner.

East Riding firewalls are switched on at all times. The local authority reviews the firewalls to ensure they are running correctly, carry out any required updates. The DSL and SBM will contact them immediately if changes are needed.

Staff and pupils are 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 have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 and above are provided with their own unique username and passwords.

Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

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

Users inform a member of the admin team if they forget their login details, who will arrange for the user to be issued with the necessary login details and password.

If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber-security Policy.

Emails

Access to and the use of emails is managed in line with the Data Protection policy and Acceptable Use policy.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use policy. Personal email accounts are not permitted to be used on the school devices. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are 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 and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Staff are reminded periodically about what a phishing email and other malicious emails might look like – this includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.

Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff and pupils can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. (See Code of Conduct). Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter

their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum. The ICT Co-ordinator & ELSA will support teachers with resources regarding E-Safety.

Concerns regarding the online conduct of any member of the school community on social media are reported to the headteacher and managed in accordance with the relevant policy, e.g. Countering-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Use of Internet Policy. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny. The Staff Code of Conduct contains information on the acceptable use of social media and staff members are required to follow these expectations at all times.

The school website

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

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information published on the school's website is kept to a minimal relating to staff and pupils. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

Use of school-owned devices

Staff members are issued with school owned devices as necessary to assist with their work. Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons. School-owned devices are used in accordance with the Device User Agreement.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are password protected. All school-owned devices are fitted with software to ensure they can be remotely accessed by our external IT Provider, in case data on the device needs to be protected, retrieved or erased.

No software, apps or other programmes can be downloaded onto a device without authorisation from the Headteacher.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

Use of personal devices

Personal devices are used in accordance with the Acceptable Use policy. Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Whistleblowing Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Whistleblowing Policy.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons.

The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Pupils' devices can be searched, screened and confiscated with reasonable cause in the presence of a member of SLT and with the knowledge of the pupil or their parent.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum

Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct, Whistleblowing Policy and Disciplinary Policy.

Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT Co-ordinator. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behavioural Policy and Child Protection and Safeguarding Policy.

Breaches and Low-level concerns will be reported and recorded via CPOMs and on the online safety tab of the safeguarding tracker. Staff will make the DSL and SBM aware of any breaches immediately. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

All online safety incidents and the school's response are recorded by the DSL.

[Section 16](#) of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video slip 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 to 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

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur. Cyberbullying will be dealt with, in the same level of appropriate consequence as found in the counter bullying policy.

Child-on-child sexual abuse and harassment

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online. Examples include the following

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse 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.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether or not 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 Protection and Safeguarding Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.
- "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school. Incidents of upskirting are reported to the DSL or headteacher who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the DSL or headteacher.

Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff. Subsequent interviews are held with the pupils involved, if appropriate.
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so. If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy. Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded. If it is necessary to view the imagery, it will not be copied, printed or shared. Viewing and deleting imagery is carried out in consultation with the headteacher and with the knowledge of the pupil and their parent.

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

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Countering Bullying Policy.

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content.

Staff members will be aware of the factors which can place pupils at increased vulnerability to radicalisation, as outlined in the Prevent training provided to all staff.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy.

Online hoaxes and harmful online challenges

The DSL will consider the potential harm to pupils of online hoaxes or challenges. A direct, targeted approach will then be pursued following the guidance for gov.uk and in line with the safeguarding children 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 pupils will be dealt with in line with the Social Emotional and Mental (SEMH) Policy.

Remote learning

All remote learning will be delivered in line with the school's Remote Education policy. This policy specifically sets out how online safety will be considered with delivering remote education.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances.

Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will consult with parents at least two weeks prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT co-ordinator and headteacher conduct half-termly light touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incident. Any changes made to this policy are communicated to all members of the school community.

Record of review/amendment

Review Date:	Sept 2024	Page No (Other info):	3, 6, 7, 11
Original: Page 3	DfE (2023) 'Keeping Children Safe in Education' Updated alongside KCSiE 2024 guidance		
Amendment:	DfE (2024) 'Keeping Children Safe in Education' Policy references added; Remote Education policy, Communication policy		
Original: Page 6	Addition to ICT co-ordinator & SBM responsibilities		

Amendment:	Ensuring that all staff have the knowledge and capability to carry out the school reporting procedure around filtering and monitoring.
Original: Page 7	• Addition to all staff members responsibilities
Amendment:	• To ensure they are the only person to access their printed material from the printer • Ensuring all online communication with parents/carers is professional and effective
Original: Page 11	• Additional information about iPad access 'Classroom Use'
Amendment:	• All iPads locked down to prevent pupils accessing inappropriate websites

Review Date:	May 2026	Page No (Other info):	
Original:	Extensive overview in line with updated DfE guidance		
Amendment:			

Appendix 1: Online harms and risks – curriculum coverage

The table below contains information about what areas of online risk schools should teach pupils about. This will be adapted to suit the age and developmental stage of Kings Mill Pupils by the ICT coordinator and Class Teachers.

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education • Sex education • Computing curriculum

Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it 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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education • Sex education • Computing curriculum • Citizenship
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed/targeted/groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	This risk or harm is covered in the following curriculum area(s): • Relationships education • Sex education • Health education • Computing curriculum
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum

Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): • Relationships education • Sex education • Computing curriculum
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum

Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum area(s): • Relationships education • Sex education • Health education • Computing curriculum • Citizenship

Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy – ‘chain letter’ style challenges	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): • Relationships education • Sex education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be ‘bots’ • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines).	This risk or harm is covered in the following curriculum area(s):

	Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	• Relationships education • Sex education
Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships	This risk or harm is covered in the following curriculum area(s): • Sex education

	• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum area(s): • Relationships education • Sex education • Computing curriculum
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): • Health education
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s): • Health education

	• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): • Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): • Sex education
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	