Beeston Fields
Flying High Academy

Online Safety Policy
2024-2025

Approved by Governing Body: Autumn 2024
Due for next review: Autumn 2025
Responsible for review: Governing Body

Policy Development

This policy has been written in consultation with the staff, parents/carers, governors and pupils of Beeston Fields. It has been approved by our Senior Leadership Team and governors. The policy will be reviewed annually and is available on our school website or from the school office.

Roles and Responsibilities

The school has a designated online safety co-ordinator, Mrs Gilbert, and an online safety governor, Laura Cameron. It is the responsibility of all adults and pupils linked to Beeston Fields to ensure that this policy is implemented fully. All staff and visitors must sign an 'Acceptable Use Policy/ICT Code of Conduct' and adhere to it at all times.

Statement of intent

Beeston Fields Primary 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 a number of 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 content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

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:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2018) Working Together to Safeguard Children
- [Updated] DfE (2023) 'Keeping children safe in education'
- DfE (2021) Sexual Violence and Sexual harassment between children in schools and colleges.
- DfE (2019) 'Teaching online safety in school' DfE (2018) 'Searching, screening and confiscation'
- Home Office (2021) Prevent Duty Guidance
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Data and E-Security Breach Prevention and Management Plan incorporated in GDP/Data Policy and Disaster Recovery Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy (Cyberbullying is incorporated)
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behavioural Policy
- Data Protection Policy
- Device User Agreement incorporated in Acceptable Use Policy
- Staff ICT and Electronic Devices Policy incorporated in Staff Acceptable Use Policy
- Prevent Duty Policy
- Pupil Remote Learning Policy

Roles and responsibilities:

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's 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 in the form of acceptable use) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The headteacher is responsible for:

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.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Overseeing the responsibility for online safety in the school, liaising closely with the online safety lead.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training and ensuring lead is trained 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 SENCO and ICT technicians.
- 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 and the platforms used.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- 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.
- Reporting to the governing board about safeguarding including online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the online safety lead, headteacher and governing board to update this policy on an annual basis.

ICT technicians (LEAD IT) are 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 headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

All staff members are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- 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.

Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Agreement 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.

The Curriculum

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

- RSE
- PSHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

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

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils of whom identify as LGBT+, pupil with SEND and LAC. We understand that some children identify as LGBT + but this does not mean that it is an inherent risk factor for harm. However, children who are LGBT+ can be targeted by other children. Relevant members of staff, e.g. the CFWS, SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

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 liaise with online safety lead to 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 and online safety lead advise 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 this 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 this policy.

Staff training

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

Online safety training for online safety lead is updated at least every 2 years and is disseminated to staff, delivered in line with advice from the three local safeguarding partners.

In addition to this training, staff also receive regular online safety updates as required and at least annually through the 39 weeks of safeguarding from the DDAT.

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.

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, LAC and LGBT+ can face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with this policy.

The DSL and online safety lead act as the first point of contact for staff requiring advice about online safety.

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. Parental awareness is raised in the following ways:

- Parents' evenings

- Parent Consultation
- Newsletters

Parents are sent a copy of the Home School Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. The Acceptable Use Policy is available on the school's website.

In the occasion a device is loaned to a student, the parent is responsible for reading, signing and following the Acceptable Use Agreement.

Classroom use

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

- Teacher Computers
- Laptops
- Tablets
- Intranet
- Cameras

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.

Internet access

Pupils, 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.

A record is kept of users who have been granted internet access in the school office.

All members of the school community are encouraged to use the school's internet network, 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 governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.

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.

The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher.

Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment.

Any changes made to the system are recorded by ICT technicians.

Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural 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 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 sections 15 and 16 of this policy.

The school's online filtering and monitoring system is provided by L.E.A.D IT. They send daily alerts to the designated staff responsible for monitoring the system.

Lead – Kristabel Beeley (Deputy Head Teacher)

Deputy Monitoring Leads – Angela Huthart and Emma Price (Office Manager)

Governor – Laura Cameron

<u>System for filtering and monitoring</u>

Everything that goes out onto the internet is filtered and monitored by a solution named iboss which is managed and maintained by LEAD IT Services. iboss provides CIPA compliant safe and secure Internet access for students and staff whenever they access the internet from school, home or wherever they may be while simultaneously protecting sensitive school data from cyberattacks including ransomware.
iboss is compliant as an Internet Watch Foundation (IWF) member and they implement the IWF blocklist, they also implement CTIRU counter-extremism blocklist. iboss follow UK Safer Internet Centres guidelines around filtering and monitoring, you can find them listed on their website under both Filtering and Monitoring providers (https://saferinternet.org.uk/resource/2021-iboss-filtering-provider-response).
Notwithstanding that no filter is 100% effective, iboss categorises and blocks the following inappropriate content. Discrimination, Drugs/Substance abuse, Extremism Malware/Hacking, Pornography, Piracy and copyright theft, Self Harm, Violence.
Whilst iboss's databases and lists are constantly updated as new threats and harmful content is identified, staff are able to log any concerns or issues to LEAD IT Services support so that the filters can be updated to mitigate any issues.
Alerts and reports relating to blocked categories are sent to designated safeguarding leads (DSL).

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians (L.E.A.D IT Services).

Firewalls are switched on at all times.

ICT technicians (L.E.A.D IT Services) review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

Staff members and pupils report all malware and virus attacks to ICT technicians (L.E.A.D IT Services).

All members of staff have their own unique usernames and private passwords to access the school's systems.

Pupils in class year are provided with their own unique username and private 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 ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.

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.

Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention and Management Plan.

Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality 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 agreement.

Personal email accounts are not permitted to be used on the school site.

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 ICT technicians.

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.

ICT technicians organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly 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.

Pupils must turn off and hand in personal devices to class teacher on arrival. Pupil's personal devices are stored away safely until the end of the school day, when returned to the pupil. Personal devices should only be brought onto school site when in the interest of the child's safety, for example if the child walks home alone.

Staff 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.

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 and assemblies.

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

Incidents that arise out of school are still acknowledged by the school, and are dealt with accordingly depending on the seriousness.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Acceptable Use 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.

Platforms for remote learning and communication with parents have been approved by Nottinghamshire County Council, namely Class Dojo and Teams. Appropriate filters are applied to ensure privacy and security.

The Staff Code of Conduct contains information on the acceptable use of social media – 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 relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the Acceptable Use Policy and Home School Agreement are met.

Use of school-owned devices

Staff members are issued with a laptop device to assist with their work.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

Students who loan a device to take home must still adhere to the measures set out in this policy. Parents are responsible for reading, signing and following Acceptable Use Agreement.

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 iPads are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material on the devices.

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

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.

Pupils must turn off and hand in personal devices to class teacher on arrival. Pupil's personal devices are stored away safely until the end of the school day, when returned to the pupil. Personal devices should only be brought onto school site when in the interest of the child's safety, for example if the child walks home alone.

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

- Toilets
- Changing rooms

Staff members are permitted to use their personal devices during lesson time to manage Dojo/Twitter and in an emergency.

Staff members may choose to use their personal devices to take photos or videos of pupils as long as they are witnessed to delete them after use.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff 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 Allegations of Abuse Against Staff Policy.

Pupils are not permitted to use their personal devices during the school day.

If a pupil needs to contact their parents during the school day, they will inform a member of staff who will contact their parent on their behalf.

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 in accordance with the Searching, Screening and Confiscation Policy.

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
- Assemblies

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, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

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 technicians.

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.

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. This policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

Cyberbullying

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

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Information about the school's full response to incidents of cyberbullying can be found in the Antibullying Policy.

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

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

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online child-on-child abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Information about the school's full response to incidents of online child-on-child abuse can be found in 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 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) 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.

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 line with the Searching, Screening and Confiscation Policy.

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, Anti-Bullying Policy and Adult Code of Conduct.

Online radicalisation and extremism

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

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

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the 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 incidents.

The next scheduled review date for this policy is November 2025.

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

Appendix 1:

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 • RSE • 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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education • RSE • Computing curriculum
	• 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	

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 • RSE • 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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
	• 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	

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 • RSE • 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 • RSE • Health education • Computing curriculum
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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
	• The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges	

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 • RSE
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). 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.	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE

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 • 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	This risk or harm is covered in the following curriculum area(s): □ RSE
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:	This risk or harm is covered in the following curriculum area(s):

	• 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	• Relationships education • RSE • 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: • 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 or missing out	This risk or harm is covered in the following curriculum area(s): □ Health education

	• 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): □ RSE
Suicide, selfharm and eating disorders	Pupils may raise topics including eating disorders, selfharm 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.	