Kingsley Primary School

Online Safety Policy

Approaches to Online Safety issues

Last updated: September 2026

Contents:

1. Statement of intent
2. Legal framework
3. School Organisation
4. Roles and responsibilities
5. Definitions
6. Managing online safety
7. The curriculum
8. Staff training
9. Educating parents
10. Classroom use
11. Internet access and use of smart technology
12. Filtering and monitoring online activity
13. Network security
14. Emails
15. Social networking
16. Generative artificial intelligence
17. The school website
18. Use of school-owned devices
19. Use of personal devices
20. Managing reports of online safety incidents
21. Responding to specific online safety concerns
22. Monitoring and review

Appendices

Appendix 1 – Online harms and risks – curriculum coverage

Appendix 2 – Online Safety Concerns

1. Statement of intent

Kingsley Primary School understands that online services underpin today's modern lifestyle. We recognise that it is essential for all pupils to gain confidence and ability in this area to prepare them for the challenge of a rapidly developing and changing technological world. In school we utilise appropriate online services in order to raise educational standards, promote pupil achievement and provide a stimulating and enjoyable environment which enables good quality teaching and learning to take place.

At Kingsley Primary School our aims are to:

- Ensure that children are online safety aware and knowledgeable about the potential dangers and personal responsibilities of using the internet both in and outside of the school environment.
- Allow staff and children to gain confidence in and enjoyment from the use of online services.
- Allow children to appreciate the relevance of the internet in our society and that they see it as an essential tool for learning, communication, finding information and for controlling and understanding the environment.
- Provide an environment where access to ICT resources is safe, natural and commonplace.
- 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 three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

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.

2. 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 (2026) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education 2026'
- DfE (2023) 'Teaching online safety in school'
- DfE (2023) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2026) 'Small Organisations Guide to Cyber Security'
- This policy operates in conjunction with the following school policies:
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Data Breach Action - GDPR
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSHE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Staff Code of Conduct (Staff Handbook)
- Behavioural Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Computing Policy
- AI Policy

3. School Organisation

Our network, systems and staff are organised to maintain the most secure environment possible.

Online Safety Teams - We have an Online Safety Policy Team which reviews and advises on our policies. A list of members is shown below. The knowledge and relevant perspective of each team member contributes to the depth and breadth of our school's policies and programmes. Due to the sensitivity of some of the issues we may need to cover, we have a separate Online Safety Management Team, providing opportunity for specific cases to be discussed and reviewed in confidence.

Management Team

- Head Teacher
- Designated Safeguarding Lead (DSL)
- Computing Coordinators

Policy Team

- Head Teacher
- Designated Safeguarding Lead (DSL)
- Computing Coordinators

- SENDCO
- Network Management
- Pastoral Care
- Other Interested Members of staff

- SENDCO
- Network Manager
- Other Interested members of staff
- Governing board
- Pupil voice
- Parent

4. Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- 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 – reviewed annually.
- 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 ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The head teacher takes ultimate responsibility for internet safety issues within the school. While delegating day to day responsibility to the Online Safety Team, the head teacher also takes specific responsibility for:

- Supporting the DSL and Team 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.
- Supporting the Online Safety Team in creating an internet safety culture within the school, including speaking to staff and pupils in support of the programme.
- 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, Team and ICT technicians to conduct 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:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- 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 SENDCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Leading in the creation and implementation of an internet safety education programme for pupils and supporting staff with information and resources as appropriate.
- Leading on the development of management protocols so that any incidents in which internet safety is breached are responded to in an appropriate and consistent manner.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Ensuring all members of the school community understand the reporting procedure.
- Developing systems and procedures for supporting and/or referring on pupils referred to them as a result of breaches of internet safety.
- Developing systems and procedures for pupils who self refer, and those pupils identified as suspected 'victims' by teaching staff.
- 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.
- Leading in the creation of a staff professional development programme that addresses both the benefits and risks of communication technologies.
- Produce written information provided with a staff use agreement.
- Ensure staff are aware that they have professional responsibilities for pupils' safety in this area.
- Reporting to the governing board about online safety on a regular basis.
- Working with the Online Safety Team to conduct termly light-touch reviews of this policy.

ICT technicians and Computing Coordinators 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 head teacher or DSL
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the Online Safety Team to conduct termly light-touch reviews of this policy.
- Conduct fortnightly reviews of virus protection and updating new where necessary.
- Providing a technical infrastructure to support internet safety practices, this includes the filtering system
- Documenting location of all internet enabled devices
- Ensuring staff laptops are secure
- Ensuring Children's notebooks are secure
- Ensuring appropriate procedures are in place for responding to online safety breaches within the school's network.
- Reporting network breaches of acceptable use of ICT facilities to the DSL

The SENDCO is responsible for

- Considering the needs of all pupils and whether the internet safety programme is appropriate to the needs of those pupils with special educational needs, or whether additional tailored materials are required
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people.
- Developing and maintaining additional policies and internet safety materials in conjunction with the Online Safety Team.
- Liaising with parents of children with special educational needs to ensure that they are aware of internet safety issues their children may encounter outside of school and offer ways in which to support them.

All staff members (including but not limited to Teachers and Teaching Assistants) are responsible for:

- Being the first point of contact in dealing with incidents of ICT misuse or abuse and may be required to act as mediators for ICT related incidents which occur inside and outside of school, such as bullying across social media and gaming.
- Implementing school AUP through effective classroom practice.
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through proper channels, reporting to the DSL and Computing coordinator in line with our school AUP.
- Planning classroom activities that embed safer internet use messages and use ICT facilities that ensure internet safety is not compromised (e.g. bookmarking and vetting websites).
- Reporting any issues with filtering and firewall procedures to the DSL and ICT technician.
- 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 up to date 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:

- Contributing to school AUP through involvement in the school's Online Safety Policy Team (pupil voice through class assemblies and open assemblies).
- 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.
- Communicating with their trusted adult about internet safety issues, and upholding any rules for safe internet use.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

5. Definitions

It is important to differentiate between *inappropriate* and *illegal* use, Procedures and sanctions also vary whether the access is *deliberate* or *accidental.* It is important to be clear about which type of incident has occurred or is suspected as the procedures differ in each case.

Outline of *inappropriate use* of the network includes accessing or possessing material that is thought to be offensive including but not limited to:

- Pornography
- Hate material
- Drug or bomb making recipes
- Sexist of racist jokes or cartoons
- Material used in a low level harassment
- Material that others may find offensive
- Defamatory, offensive, abusive, indecent or obscene
- Material used in breach of confidence, privacy, trade secrets.

Outline of *Unlawful or Illegal use* of the network includes accessing or possessing material that contains (This is not an exclusive list. There may be other information that is deemed to be illegal):

- Direct threats of physical harm
- Child abuse images
- Incitement to racial hatred or violence
- Copyrighted trademarked and other proprietary material used without proper authorisation.

6. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Class assemblies are conducted at least fortnightly on the topic of remaining safe online

Handling online safety concerns

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

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

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

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. If the concern is about the headteacher, it is reported to the chair of governors.

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, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

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

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

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

7. The curriculum

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

- RSHE
- Health education
- PSHE
- Citizenship
- 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
- How to identify that online abuse and offline abuse are often directly linked

Knowledge and behaviours that are covered in the government's online media literacy strategy

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

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 with SEND and LAC. Relevant members of staff, e.g. the SENDCO 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. 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 Child Protection and Safeguarding Policy.

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

8. Staff training

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.

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. Online safety training for staff is updated and delivered annually. In addition to this training, staff also receive regular online safety updates as required and at least annually.

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.

All staff are signposted to 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.

9. 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
- Newsletters

Parents are sent a paper copy of the Acceptable Use Agreement ('Home School Agreement') when their child joins Kingsley Primary school and guided to where it is accessed online. They are encouraged to go through this with their child each year to ensure their child understands the document and the implications of not following it.

10. Classroom use

A wide range of technology is used during lessons, including (but are not limited to) the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Video cameras
- iPads
- Kindles
- EasiSpeak Dictaphones

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.

11. Internet access and use of smart technology

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 when using a school device, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

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

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

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

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

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

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

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

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

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

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

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

12. Filtering and monitoring online activity

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

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs and highlight the importance of escalating these issues to the DSL when online concerns arise.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be 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. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or

materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be 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 Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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

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

13. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff members and pupils report all malware and virus attacks to ICT technician and Computing Coordinator. All members of staff have their own unique usernames and private passwords to access the school's systems.

- Pupils are provided with their own unique username and passwords.
- Staff members and pupils are responsible for keeping their passwords private.
- Staff passwords have a minimum and maximum length and require a mixture of letters and numbers 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.
- Full details of the school's network security measures can be found in the Data Breach Action.

14. 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 KS2 pupils are given approved school email accounts and are to only use these accounts at school and when doing school-related work outside of school hours using Google Classrooms.

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 using school devices.

Any email that contains sensitive or personal information is only sent using secure and encrypted email.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

15. 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 can use personal social media during break and lunchtimes on their own devices; however, inappropriate or excessive use of personal social media during school hours may result in further action.
- Staff receive regular training on how to use social media safely and responsibly and 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 over social networking sites and are reminded to alter their privacy settings to ensure pupils 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.
- 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.

Use on behalf of the school

- The school's official social media channels are only used for official educational or engagement purposes.
- Staff members must be authorised by the head teacher 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 – staff members are required to follow these expectations at all times.

16. Generative artificial intelligence (AI)

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

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

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

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

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Please refer to the school AI Policy for more detail here.

17. The school website

The head teacher 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 Photography Policy are met.

18. Use of school-owned devices

Teachers are issued with a school laptop to assist their work.

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

All school-owned devices are password protected.

ICT technicians review all school-owned devices on an annual 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 or Computing Coordinator.

19. Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency unless otherwise agreed. Adults are encouraged to take their mobile phone with them during a fire drill and have them on hand in the event of a ‘lockdown’ procedure.

Staff members report concerns about their colleagues’ use of personal devices on the school premises in line with the Whistle Blowing 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 head teacher will inform the police and action will be taken in line with Disciplinary Policy and Procedure.

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

If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office.

The head teacher 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 documentation is provided 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.

20. 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 head teacher 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 head teacher 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 head teacher contacts the police.

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

21. Responding to specific online safety concerns

Please also refer to Safeguarding Policy, specifically Contextual Safeguarding.

Further details of these Online Safety Concerns can be found in Appendix 2 of this policy

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 Anti bullying Policy.

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:

- 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 peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online peer-on-peer 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 peer-on-peer 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)

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.

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 head teacher 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 and Anti Bullying Policy

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.

Misinformation, disinformation, conspiracy theories, deepfake technology and AI-generated content

The school recognises emerging online risks including misinformation, disinformation, conspiracy theories, deepfake technology and AI-generated content. Pupils will be taught to critically evaluate digital information and to understand the potential risks associated with emerging technologies. Staff will receive appropriate training to support pupils in navigating these online environments safely

22. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the head teacher conduct termly light-touch reviews of this policy to evaluate its effectiveness. The governing board, head teacher 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 September 2026.

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

Appendix 1: Online harms and risks – curriculum coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance and underpins our Online Safety Curriculum in school.

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): PSHE Computing curriculum Project Evolve Assemblies
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 PSHE Computing curriculum Project Evolve Assemblies
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 (Fake news) 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 PSHE Computing curriculum Project Evolve Assemblies
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.	This risk or harm is covered in the following curriculum area(s):

	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	Relationships education PSHE Computing curriculum Project Evolve Assemblies
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 Project Evolve Assemblies
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 Project Evolve Assemblies
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 Computing curriculum Project Evolve Assemblies

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): PSHE Computing curriculum Project Evolve Assemblies
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 Project Evolve Assemblies
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): PSHE Computing curriculum Project Evolve Assemblies
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 PSHE Computing curriculum Project Evolve Assemblies

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 PSHE Project Evolve Assemblies
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 PSHE Project Evolve Assemblies
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 Project Evolve Assemblies
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	This risk or harm is covered in the following curriculum area(s): Relationships education PSHE Computing Curriculum Project Evolve Assemblies

	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.	
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 Computing Curriculum Project Evolve Assemblies
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 Computing curriculum Project Evolve Assemblies
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	This risk or harm is covered in the following curriculum area(s):

	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	PSHE Project Evolve Assemblies
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 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	This risk or harm is covered in the following curriculum area(s): Health education Computing Curriculum PSHE Project Evolve Assemblies
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 Computing Curriculum Project Evolve Assemblies
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.	

Appendix 2: Online Safety Concerns

Cyberbullying

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

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.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

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

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

Grooming and exploitation

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

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

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

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

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

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

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

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

Radicalisation

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

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

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

Mental health

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

Online hoaxes and harmful online challenges

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

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

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

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

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

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

- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

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

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

Cyber-crime

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

Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

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

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.