Hunsbury Park Primary School

Online Safety Policy and Procedure

Last updated: September 2021

Contents:

Appendices

a) Online Safety Activities and Issues
b) Useful Resources for Teachers and Parents
c) Response to an Incident of Concern Flowchart
d) Staff and Governor Acceptable Use Agreement
e) Acceptable Use Agreement: Pupils (KS1)
f) Acceptable Use Agreement: Pupils (KS2)
g) Visitor Acceptable Use Agreement
h) Rules for EYFS and KS1
i) Rules for KS2
j) Online Harms and Risks Curriculum Coverage

Statement of Intent

Hunsbury Park 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 three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, 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.

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4/5G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets, mobile phones and toys mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an Online Safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL, classroom teachers, support staff, young people or parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

Online Safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An Online Safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.

- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective Online Safety programme.

Above all, Online Safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

1.2. This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Data and E-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Staff Code of Conduct
- Behavioural Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Device User Agreement

- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Pupil Remote Learning Policy

2. Roles and responsibilities

2.1. 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, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

2.2. 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.

2.3. 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.

SAFEGUARDING INFORMATION

All children have a right to be protected from harm and all adults have a role to play in ensuring that our children are protected and safe.

As individuals, we all play an important part in the child protection process.

Whether as part of your job or volunteering activities, or simply as a member of your local community, child protection is everyone's responsibility.

The Designated Safeguarding Lead Teachers at Hunsbury Park are:

Mrs Riley
Designated Safeguarding Lead

Safeguarding Team

Mrs Burton
Deputy Designated Safeguarding Lead

Mr York
Deputy Designated Safeguarding Lead

Our Safeguarding Team are easily identified by their orange lanyards

If you have any concerns about the welfare of a pupil while working in or visiting our school, please speak to one of the DSLs immediately. You will be asked to complete and sign a "Cause for Concern" form. You can also contact the Multi-Agency Safeguarding Hub team directly on: *0300 126 1000*

- 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 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping 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 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 headteacher and governing board to update this policy on an annual basis.

2.4. ICT technicians 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.

2.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- 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.

2.6. 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 have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

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

- The curriculum and the school's approach to online RSE
- Health education
- PSHE
- Citizenship
- Computing

3.2. 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.

3.3. 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.

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

3.5. 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 when something is deliberately deceitful or harmful

- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

3.6. 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 in the appendices of this policy.

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

3.8. 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 SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

3.9. 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?

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

3.11. 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.

3.12. 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.

3.13. 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 asking questions, and are not worried about getting into trouble or being judged.

3.14. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 23 and 24 of this policy.

3.15. 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 sections 23 and 24 of this policy.

4. Teaching and learning (the wider curriculum)

Why the internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

Staff model safe and responsible behaviour in their use of technology during lessons.

Teachers remind pupils about their responsibilities through an end-user Pupil Acceptable Use Agreement which every pupil will sign when they log on to the school network.

Internet use will enhance learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant internet content to the Designated Safeguarding Leader (DSL). This can be done anonymously, or in person, and will be treated in confidence.

The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.

- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files – without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

5. Introducing the Online Safety Policy to pupils

5.1. Online Safety rules and guidance posers will be displayed in every classroom, corridors and the computing suite and discussed with pupils regularly.

5.2. Children will be taught about this online safety policy and the importance of safeguarding at the beginning of the school year. Following this the children will then sign the pupil acceptable use agreement before taking it home for their parents to also discuss with them and return to school. These agreements will be stored in the online safety folder held by the DSL.

Pupils will be informed that network and internet use will be monitored and appropriately followed up.

A programme of training in online safety will be developed by the Computing subject leader, PSHE subject leader and DSL.

Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

6. Staff training

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

6.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners.

6.3. In addition to this training, staff also receive regular online safety updates as required and at least annually.

6.4. 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.

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

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

6.6. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy as they occur by the Designated Safety Lead.

6.7. 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.

6.8. All staff are informed about how to report online safety concerns, in line with sections 23 and 24 of this policy.

6.9. The DSL acts as the first point of contact for staff requiring advice about online safety.

7. Educating parents

7.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.

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

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

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

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

This takes the form of a regular post on ClassDojo using the 'Wake Up Wednesday' online safety information posters downloaded from the National Online Safety website as and when appropriate to.

7.5. Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

7.6. Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Online resources
- Information sent via ClassDojo

8. Classroom use

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

- Desktop computers
- Laptops
- Email

8.2. 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.

8.3. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

9. Internet Access

9.1. Pupils, staff, governors, visitors 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.

9.2. A record is kept of users who have been granted internet access in the school office and in the DSL's online safety folder.

9.3. 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.

10. Filtering and Monitoring Online Activity

10.1. The head teacher ensures the school's ICT network has appropriate filters and monitoring systems in place.

10.2. The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.

10.3. 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.

10.4. 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.

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

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

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

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

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

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

10.11. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy.

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

10.13. 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.

10.14. The school's network and school-owned devices are appropriately monitored.

10.15. All users of the network and school-owned devices are informed about how and why they are monitored.

10.16. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 23 and 24 of this policy.

11. Network security

11.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

11.2. Firewalls are switched on at all times.

11.3. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

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

11.5. Staff members and pupils report all malware and virus attacks to ICT technicians.

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

11.7. Pupils in class year or key stage and above are provided with their own unique username and private passwords.

11.8. Staff members and pupils are responsible for keeping their passwords private.

11.9. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

11.10. Passwords expire after **90** days, after which users are required to change them.

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

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

11.13. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.

11.14. 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.

12. Emails

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

12.2. 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.

12.3. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement.

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

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

12.6. Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians.

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

12.8. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

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

12.10. The school does not publish personal email addresses of pupils or staff on the school website.

13. Social networking

Personal use

13.1. Access to social networking sites is filtered as appropriate.

13.2. Staff and pupils are not permitted to use social media for personal use during the school day.

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

13.4. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

13.5. Staff are encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites as stated on the school's 'Code of Conduct' policy.

13.6. Staff receive annual training on how to use social media safely and responsibly.

13.7. 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.

13.8. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

13.9. Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

13.10. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

13.11. Pupils will be advised to use nicknames and avatars when using social networking sites.

13.12. 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

13.13. The use of social media on behalf of the school is conducted in line with the Social Media Policy.

13.14. The school's official social media channels are only used for official educational or engagement purposes.

13.15. Staff members must be authorised by the headteacher to access to the school's social media accounts.

13.16. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

13.17. 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.

14. Online hoaxes and harmful online challenges

14.1. 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.

14.2. 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.

14.3. The DSL ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with section 3 of this policy.

14.4. The DSL will work with the SENCO to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

14.5. The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes, e.g. by displaying posters.

14.6. 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.

14.7. 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.

14.8. 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.

14.9. The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

14.10. The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

14.11. Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, 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 even to individual children at risk where appropriate.

14.12. 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.

14.13. 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:

- Factual and avoids 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 that 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.
- Age-appropriate and appropriate for the relevant pupils' developmental stage.
- Supportive.
- In line with section 23 and section 24of this policy.

15. The school website

15.1. 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 following statutory DfE guidelines for publications:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

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

15.3. Personal information relating to staff and pupils is not published on the website.

15.4. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

15.5. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

15.6. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

15.7. Uploading of information is restricted to our website authorisers.

15.8. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

15.9. The point of contact on the website is the school address and telephone number.

15.10. Photographs published on the web do not have full names attached.

15.11. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

16. Publishing Pupils' Images and Work Online

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The school will consider using group photographs rather than full-face photos of individual children.

Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

Written permission from parents will be obtained before photographs of pupils are published on the school website or Class DoJo.

Work can only be published with the permission of the pupil and parents.

Pupil image file names will not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

Staff sign the school's Staff and Governor Acceptable Use Agreement annually, this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.

The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

Pupils are taught about how images can be manipulated in their e-safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

17. Use of school-owned devices

17.1. Staff members are issued with the following devices to assist with their work:

- Laptop
- iPad

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

17.3. School-owned devices are used in accordance with the Device User Agreement.

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

17.5. All school-owned devices are password protected.

17.6. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

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

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

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

17.10. Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

18. Use of personal devices

18.1. Personal devices are used in accordance with the Staff ICT and Electronic Devices Policy and the Pupils' Personal Electronic Devices Policy.

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

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

- Toilets
- Changing rooms
- Classrooms
- Areas of the school where pupils are present

18.4. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency and agreed by the head teacher.

18.5. Staff members are not permitted to use their personal devices to take photos or videos of pupils, unless agreed by the head teacher.

18.6. 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.

18.7. 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.

18.8. Pupils are not permitted to use their personal devices in school. If they have a personal device (this includes watches with photographic capabilities), this must be given to the class teacher who will keep it safe and return it to the pupil at the end of the school day.

18.9. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office after seeking permission from their class teacher and the head teacher.

18.10. Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

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

18.12. Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy.

18.13. 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.

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

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

The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded.

The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

The Bluetooth, or similar function, of a mobile phone will be switched off at all times and not be used to send images or files to other mobile phones.

No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Staff handheld devices, including mobile phones and personal cameras, must be noted in school – name, make and model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, unless permission has been granted by the head teacher and they must withhold their telephone number by inputting '141' before dialing the number.

Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods, unless permission has been granted by a member of the SLT in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, it will only take place when approved by the SLT.

Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose as stated in the school's photography policy

If a member of staff breaches the school policy, disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Pupils will abide by the following rules when using personal devices in school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety; this will need to be agreed by a member of SLT in advance and handed into the school office.
- If a pupil breaches the school policy, the phone or device will be confiscated immediately and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school policy.
- If a pupil needs to contact their parents, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupil should bring their mobile phone or personally-owned device into school without consent from a member of SLT. Any device brought into school without permission will be confiscated.

19. Managing Emerging Technologies

19.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones will be strictly prohibited.

Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

20. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

21. Authorising internet access

21.1. All staff will read and sign the Staff and Governor Acceptable Use Agreement before using any school ICT resource.

21.2. All children and their parents/carers will read and sign the Pupil Acceptable Use Agreement before using any school ICT resource. These are differentiated for Early Years/Key Stage One and Key Stage Two.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. The signed forms will be kept in the online safety folder kept by the Designated Safety Lead.

At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

Any person not directly employed by the school will be asked to read and sign the Visitor Acceptable Use Agreement being allowed to access the internet from the school site.

22. Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.

The school should audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

23. Managing reports of online safety incidents

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

- Staff training
- The online safety curriculum, which is taught as part of the school's computing curriculum.

23.2. 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.

23.3. 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.

23.4. 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.

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

23.6. 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.

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

23.8. Section 17 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

24. Responding to specific online safety concerns

Cyberbullying

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

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

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

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

24.4. 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

24.5. 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.

24.6. 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.

24.7. 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

24.8. 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.

24.9. 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.

24.10. "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

24.11. Upskirting is not tolerated by the school.

24.12. 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.

Sexting and the sharing of indecent imagery of pupils

24.13. Sharing indecent 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.

24.14. Staff will receive appropriate training regarding child sexual development and will understand the difference between sexual behaviour that is considered normal and developmentally expected, and sexual behaviour that is inappropriate and/or harmful.

24.15. All concerns regarding sexting are reported to the DSL.

24.16. The DSL will use their professional judgement, in line with the Child Protection and Safeguarding Policy, to determine whether the incident is **experimental**, i.e. expected for the developmental stage of the pupils involved, or **aggravated**, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the pupil depicted.

24.17. Where the incident is categorised as 'experimental', the pupils involved are supported to understand the implications of sharing indecent imagery and to move forward from the incident.

24.18. Where there is reason to believe the incident will cause harm to the pupil depicted, or where the incident is classified as 'aggravated', 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

24.19. When investigating a report, staff members will not view and nude and semi-nude images unless there is a good and clear reason to do so.

24.20. If a staff member believes there is a good reason to view nude or semi-nude imagery as part of an investigation, they discuss this with the DSL and headteacher first.

24.21. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

24.22. If a decision is made to view the imagery, the DSL will be satisfied that viewing:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any pupil involved.
- Is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the pupil in taking down the image or in making a report.
- Is unavoidable because a pupil has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.

24.23. Where it is necessary to view the imagery the DSL will:

- Never copy, print, share, store or save images; this is illegal.
- Discuss the decision with the headteacher.
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team with delegated authority from the headteacher.
- Make sure viewing takes place with the headteacher or another member of the SLT in the room; additional people in the room will not view the imagery.
- Only view the imagery on the school premises.
- Record how and why the decision was made to view the imagery in line with the Record Management Policy and the Child Protection and Safeguarding Policy.
- Make sure that images are viewed by a member of staff of the same sex as the pupil, where appropriate.
- Ensure that, if devices need to be passed on to the police, the device is confiscated, disconnected from Wi-Fi and data and turned off immediately to avoid imagery being accessed remotely; the device will be secured until it can be collected by police.

24.24. Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the DSL's professional judgement.

24.25. Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.

24.26. Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

24.27. Viewing and deleting imagery is carried out in line with the Searching, Screening and Confiscation Policy.

Online abuse and exploitation

24.28. 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.

24.29. 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.

24.30. 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

24.31. The school does not tolerate online hate content directed towards or posted by members of the school community.

24.32. 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

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

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

25. Remote learning

25.1. All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

25.2. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.

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

25.3. All staff and pupils using audio communication must:

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

25.4. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

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

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

25.7. In the instance that remote learning is necessary, the school will inform parents about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

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

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

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

- Reinforce the importance of children staying safe online.

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

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

26. Monitoring and review

26.1. 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.

26.2. The governing board, headteacher, DSL, deputy DSL's and the Computing Lead will review this policy in full on an annual basis and following any online safety incidents.

26.3. The next scheduled review date for this policy is September 2022.

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

Online Safety Activities and Issues

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites	• Parental consent should be sought • Pupils should be supervised • Pupils should be directed to specific, approved online materials
Using search engines to access information from a range of websites	• Filtering must be active and checked frequently • Parental consent should be sought • Pupils should be supervised • Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with
Exchanging information with other pupils and asking questions of experts via email or blogs	• Pupils should only use approved email accounts or blogs • Pupils should never give out personal information
Publishing pupils' work on school and other websites	• Pupil and parental consent should be sought prior to publication • Pupils' full names and other personal information should be omitted • Pupils' work should only be published on moderated sites and only by the school administrator.
Publishing images, including photographs of pupils	• Parental consent for publication of photographs should be sought • Photographs should not enable individual pupils to be identified • File names should not refer to the pupil by name • Staff must ensure that published images do not breach copyright laws
Communicating ideas within chat rooms or online forums	• Only chat rooms dedicated to educational use and that are moderated should be used • Access to other social networking sites should be blocked • Pupils should never give out personal information
Audio and video conferencing to gather information and share pupils' work	• Pupils should be supervised • The school should only use applications that are managed by LAs and approved educational suppliers
Social networking	• Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents • Social networking sites should be blocked on the school network • Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online

Useful Resources for Teachers and Parents

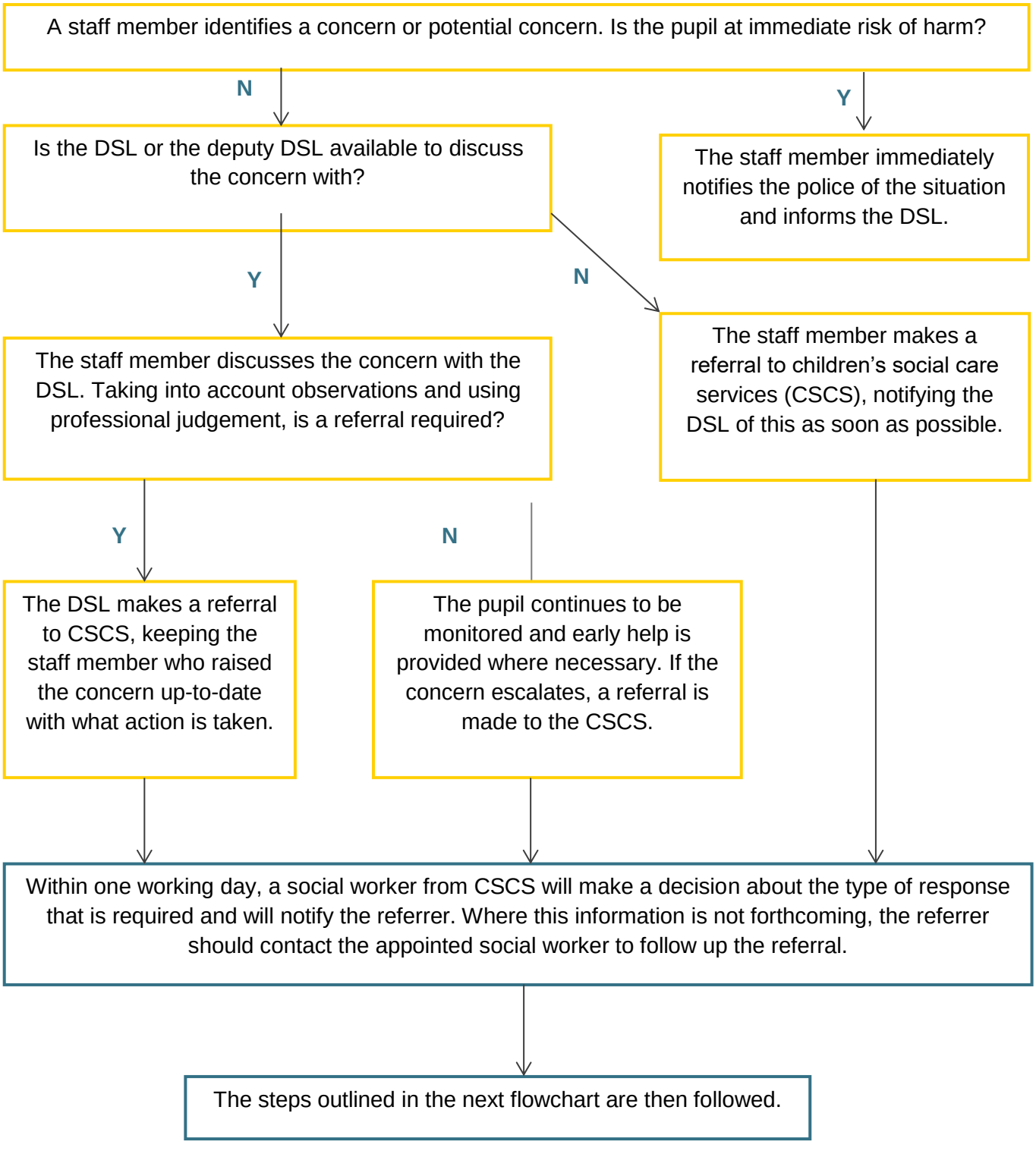
Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school
Project Evolve	www.projectevolve.co.uk
Be Internet Legends	https://beinternetlegends.withgoogle.com/en_uk/parents/

Response to an Incident of Concern Flowchart

The process outlined within the first section should be followed where a staff member has a safeguarding concern about a child. Where a referral has been made, the process outlined in the 'After a referral is made' section should be followed.

The actions taken by the school are outlined in yellow, whereas actions taken by another agency are outlined in blue.

Before a referral is made



After a referral is made

Once a referral has been made, a social worker from CSCS will notify the referrer that a decision has been made and one of the following responses will be actioned.

The pupil is in need of immediate protection.

Where the pupil is at risk of significant harm but is not in immediate danger, a strategy discussion is held.

No formal assessment is needed.

Where appropriate to do so, the DSL and staff member who raised the concern may be consulted during these stages to ensure that all areas of concern are addressed.

The DSL supports the initial staff member to liaise with other agencies to arrange an early help assessment and appropriate support.

Appropriate emergency action is taken by the social worker, police or NSPCC.

A Child in Need assessment is completed within 45 working days.

Within 15 working days of the strategy discussion, an initial child protection conference is held.

A child protection plan is potentially required.

The type of support needed is identified, arranged through multi-agency liaison and provided effectively.

Staff keep the pupil's circumstances under review and re-refer if appropriate to ensure circumstances improve – the pupil's best interests always come first.

If the child's situation does not appear to be improving, the DSL should press for re-consideration to ensure their concerns have been addressed and, most importantly, that the child's situation improves.

Staff and Governor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.
- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed)

Upon the reading and completion of this policy, please return it to the school office.

Acceptable Use Agreement: Pupils (KS1)

Child's Name: _____

Class: _____

Year: _____

Pupil Acceptable Use Agreement

I will:

	SPEAK If you see something you do not like, speak to an adult.
	ASK Ask permission from an adult before you use the internet.
	FRIENDS Friends are people we know, we do not speak to people we do not know.
	ENJOY Enjoy, have fun and be safe.

Pupil Signature: _____

Date: _____

Parent / Carer Signature

As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my son /daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

If at any time you have any concerns regarding online safety, please contact the Designated Safety Lead via the school office on 01604 761566 or email criley@hunsburypark.org.

Name of Parent: _____

Parent Signature: _____

Date: _____

Acceptable Use Agreement: Pupils (KS2)

Child's Name: _____

Class: _____

Year: _____

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- If relevant, I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the learning platform, school network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my safety.
- I will not bring a mobile phone or other personal ICT device into school.

Pupil Signature: _____

Date: _____

Parent / Carer Signature

As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my son /daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

If at any time you have any concerns regarding online safety, please contact the Designated Safety Lead via the school office on 01604 761566 or email criley@hunsburypark.org.

Name of Parent: _____

Parent Signature: _____

Date: _____

Hunsbury Park Primary School

Visitor Acceptable Use Agreement

Last updated: September 2021

Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. Our online safety policy is to help ensure that all visitors are aware of their professional responsibilities when using any form of ICT and to help keep everyone safe. All visitors are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher, the designated safety lead, or one of the deputy safety designated leads or the computing lead.

Please read the terms and conditions below, if you agree to abide by these, please sign and hand into the office, where you will be given the details to access the school wifi information.

- I will only use my professional email account, internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with staff and others outside of the school are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils or staff.
- I will only use the approved email system for any communications with parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to the office who will inform the computing lead and the designated safety lead.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.

- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Once I have completed my visit at Hunsbury Park Primary School, I will delete all information, including the Wi-Fi login from my device/s.
- If at any time you have any concerns regarding online safety, please contact the Designated Safety Lead via the school office on 01604 761566 or email criley@hunsburypark.org.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed)

Upon the reading and the completion of this form, please hand this to a member of the school office who will inform you of the information required.

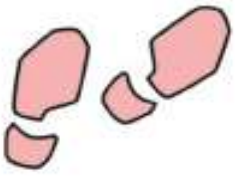
Rules for EYFS and KS1

Think then Click

These rules help us to stay safe on the internet

E-safety rules for EYFS and KS1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.




Rules for KS2

Think then Click

These rules help us to stay safe on the internet

E-safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.




Online harms and risks – curriculum coverage

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 • That the widespread nature of this sort of content can often appear to be a stamp of	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education • RSE • Computing curriculum

	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 • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum

Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): • Relationships education • 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 • The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): • Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s):

	• 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	• 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
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

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): • **[Secondary schools]** 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: • 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 • 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): • **[Secondary schools]** Health education
Impact on quality of life, physical and mental health	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.	This risk or harm is covered in the following curriculum area(s):

and relationships	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	• Health education
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): • **[Secondary schools]** RSE
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.	