The Devonshire Hill Nursery & Primary School
Online Safety Policy

Statement of Intent

The Devonshire Hill Nursery & 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.

Ratification date: 23rd September 2020	Review date: As required
This policy is reviewed as required by the designated safeguarding lead, school business manager and headteacher, then ratified by governing body	
Headteacher	Chair of Governors

Contents:

Appendices:

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 General Data Protection Regulation (GDPR)*
- *Data Protection Act 2018*
- *DfE (2020) 'Keeping children safe in education'*
- *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'*
- *UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'*

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

- *Anti-bullying Policy*
- *Data Protection Policy*
- *Disciplinary Procedure (including Code of Conduct)*
- *Information Security Policy*
- *Managing Allegations Against Staff Policy*
- *Photography Policy*
- *Pupil Behaviour and Discipline Policy*
- *Relationships and Sex Education Policy*
- *Remote Learning Policy*
- *Safeguarding and Child Protection Policy*
- *Whistleblowing Policy*

2. Roles and responsibilities

2.1. The governing body 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 as required in line with new guidance.
- 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.

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 SBM to conduct regular light-touch reviews of this policy.
- Working with the DSL, SBM and governing body to update this policy on an as required in line with updated guidance.

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.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and ICT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- 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 headteacher about online safety on a regular basis so this can be included in safeguarding reporting to the governing body.
- Working with the headteacher and SBM to conduct regular light-touch reviews of this policy.
- Working with the headteacher and governing body to update this policy on as required in line with guidance updates.

2.4. The SBM is responsible for:

- Arranging and overseeing 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 regular light-touch reviews of this policy.

2.5. All staff members are responsible for:

- Adhering to the *Acceptable Use Agreement* (Appendix A) 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 appropriate *Acceptable Use Agreement* (Appendix B or C) and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

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

- PSHE
- Relationships & Health Education (Jigsaw)
- Computing

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

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

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 *Appendix D* 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, 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 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 15 and 16 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 14 and 5 of this policy.

4. Staff training

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

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

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

4.4. The DSL and 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.

4.5. 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.

4.6. All staff must read this policy as part of their induction and are informed of any changes to the policy.

4.7. Staff are required to adhere to the staff Code of Conduct and Acceptable Use Agreement, which includes provisions for the acceptable use of technologies and the use of social media.

4.8. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

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

5. Educating parents

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

5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Newsletters
- Parent/carer workshops
- Parents' evenings

5.3. Parents/carers are provided with a copy of the appropriate *Acceptable Use Agreement* (Appendix B or C) on admission and when their children move into another phase. Parents/carers are encouraged to go through the agreement with their child to ensure they understand the document and the implications of not following it.

6. Classroom use

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

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

6.2. 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.

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

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

7. Internet Access

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

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

7.3. 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.

8. Filtering and monitoring online activity

8.1. The governing body ensures the school's ICT network has appropriate filters and monitoring systems in place.

8.2. The school uses London Grid for Learning (LGfL) for broadband and filtering systems. Only members of the SLT, with the headteacher's agreement, may authorise access to blocked sites.

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

8.4. The school's ICT consultant makes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.5. Requests regarding making changes to the filtering system are directed to the members of the SLT and must be agreed by the headteacher.

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

8.7. Reports of inappropriate websites or materials are made to the SBM immediately, who investigates the matter and ensures any necessary changes are made.

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

8.9. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the *Pupil Behaviour and Discipline Policy.*

8.10. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the *Employee Disciplinary Procedure*.

8.11. 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.

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

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

8.14. Concerns identified through monitoring are reported to the DSL (via the SBM) who manages the situation in line with sections 14 and 15 of this policy.

9. Network security

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

9.2. Firewalls are switched on at all times.

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

9.4. Staff and pupils are not able to download unapproved software and are advised not to open unfamiliar emails or any attachments.

9.5. Staff members and pupils report all malware and virus attacks to the SBM, or to the SBM via a responsible adult.

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

9.7. Pupils (or their parents/carers) are provided with their own unique username and private passwords.

9.8. Staff members and pupils/parents/carers are responsible for keeping their passwords private.

9.9. Passwords have a minimum and maximum length and require a mixture of letters and numbers to ensure they are secure.

9.10. Passwords expire after 180 days, after which users are required to change them.

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

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

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

9.14. 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.

9.15. Full details of the school's network security measures can be found in the *Information Security Policy*, part of a suite of *Data Protection Policies.*

10. Emails

10.1. Access to and the use of emails is managed in line with the *Data Protection Policies* and *Acceptable Use Agreement.*

10.2. 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.

10.3. Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.

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

10.5. Any email that contains sensitive or personal information must be risk assessed and sent securing if risk is considered high.

10.6. Staff members and pupils are should block spam and junk mail where this is not captured by the filtering system. Concerns should be reported to the SBM or DSL.

10.7. Chain letters, spam and all other emails from unknown sources must be deleted without being opened.

11. Social networking

Personal use

11.1. Access to social networking sites over the school network is restricted.

11.2. Staff are not permitted to use social media for personal use during lesson time.

11.3. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in disciplinary action.

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

11.5. 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.

11.6. 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.

Use on behalf of the school

11.7. The use of social media on behalf of the school must be authorised by the headteacher.

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

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

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

11.11. 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.

12. The school website

12.1. 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.

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

12.3. Personal information relating to staff and pupils is not published on the website unless there is a legal basis to do so.

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

13. Use of school-owned devices

13.1. Staff members may be issued with the following devices to assist with their work:

- Tablet
- Laptop
- Mobile phone

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

13.3. School-owned devices are used in accordance with the *Acceptable Use Agreements.*

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

13.5. All school-owned devices must be password or passcode protected.

13.6. 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.

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

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

13.9. Staff members or pupils found to be misusing school-owned devices are disciplined in line with the *Employee Disciplinary Procedure* and *Pupil Behaviour and Discipline Policy.*

14. Use of personal devices

14.1. Personal devices are used in accordance with the employee *Code of Conduct* and *Acceptable Use Agreement*.

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

14.3. Pupils are not permitted to bring personal devices to school. Unauthorised devices will be confiscated and parents/carers contacted informing them of the action and advised of the school's policy.

14.4. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

14.5. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

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

14.7. 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 *Managing Allegations Against Staff Policy*.

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

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

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

14.11. 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.

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

14.13. Any concerns about visitors' use of personal devices on the school premises are reported to a member of the Senior Leadership Team.

15. Managing reports of online safety incidents

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

- Computing curriculum
- PSHE
- Relationships & Health Education

15.2. 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*, *Managing Allegations Against Staff Policy* and *Employee Disciplinary Procedures*.

15.3. Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members.

15.4. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. *Pupil Behaviour and Discipline Policy* and *Safeguarding and Child Protection Policy*.

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

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

15.7. Section 15 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

16. Responding to specific online safety concerns

Cyberbullying

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

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

16.3. Information about the school's full response to incidents of cyberbullying can be found in the *Anti-bullying Policy*.

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

16.4. 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

16.5. 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.

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

16.7. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the *Safeguarding and Child Protection Policy*.

Upskirting

16.8. 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.

16.9. 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.

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

16.11. Upskirting is not tolerated by the school.

16.12. 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 *Safeguarding and Child Protection Policy.*

Youth produced sexual imagery (sexting)

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

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

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

- The DSL holds an initial review meeting with appropriate school staff.
- Subsequent interviews are held with the pupils involved, if appropriate.
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm.
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately.
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented.
- When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

- If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.
- The decision to view imagery is based on the professional judgement of the DSL and always complies with the *Safeguarding and Child Protection Policy*.
- Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.
- If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

16.16. 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.

16.17. 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.

16.18. 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 *Safeguarding and Child Protection Policy*.

Online hate

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

16.20. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. *Staff Code of Conduct* and *Anti-Bullying Policy.*

Online radicalisation and extremism

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

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

17. Remote learning

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

17.2. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted.
- 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.

17.3. 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.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

17.4. The school will consider whether one-to-one sessions are appropriate in exceptional circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by SENDCo in collaboration with the Headteacher as the school's DSLs.

17.5. Pupils not using devices or software as intended will be disciplined in line with the *Pupil Behaviour and Discipline Policy.*

17.6. 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.

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

17.8. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed and can establish secure connections.

17.9. The school will advise parents/carers 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.

17.10. 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.

17.11. 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.

18. Monitoring and review

18.1. The school recognises that the online world is constantly changing; therefore, the DSL, SBM and headteacher will conduct regular light-touch reviews of this policy to evaluate its effectiveness.

18.2. The governing body, headteacher and DSL will review this policy following any online safety incidents or changes in guidance.

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

Acceptable Use Agreement: All Staff, Volunteers and Governors

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will *not* be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff (including agency staff), volunteers and governors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. Using technology in school

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher or business manager.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information, or perform any school business.
- I will not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored and destroyed in line with the GDPR.
- Delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless permitted to do so by the headteacher or school business manager.
- I will report immediately any concern about the effectiveness of anti-virus protection on any school-owned device.
- I will not use removable media devices such as USB memory sticks and external hard drives where avoidable.
- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised and delete immediately when not needed.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that personal mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.

- I will not use personal mobile devices to take images or videos of pupils or staff.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not use the WiFi system to access any inappropriate or illegal content.
- I will not use personal or school-owned mobile devices to communicate with pupils or parents, unless explicitly agreed by the headteacher.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from parents/carers of individual(s) in the images or videos.
- I will ensure that any school data stored on mobile devices is stored no longer than necessary and archived/destroyed as appropriate and in accordance with the *Data Retention Policy*

3. Social media and online professionalism

- If I am representing the school online (e.g. through blogging or on school social media account) I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the headteacher before any personal data is transferred to a personal device.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has adequate security and anti-virus software before undertaking any home-working.

- I will ensure no unauthorised persons, such as family members or friends, have access to school systems and data via personal devices used for home-working.
- I will act in accordance with the school's *Information Security Policy* when transporting school equipment and data.

5. Training

- I will ensure I participate in any online safety training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the *Online Safety Officer* to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the headteacher.
- I understand that my use of the internet will be monitored by the *Online Safety Officer* and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me in accordance with the *Employee Disciplinary Procedure*, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signature: _____ Date: _____

Print name: _____

Head's signature: _____ Date: _____

Print name: _____

The Devonshire Hill Nursery and Primary School
Successful Learners

Acceptable Use Agreement for Key Stage 1

Think before you click

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

The Devonshire Hill Nursery and Primary School
Successful Learners

Acceptable use Agreement for Key Stage 2

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework;
- I will only edit or delete my own files and not look at, or change, other people's files without their permission;
- I will keep my logins and passwords secret;
- I will not bring files into school without permission or upload inappropriate material to my workspace;
- I am aware that some websites and social networks have age restrictions and I should respect this;
- I will not attempt to visit Internet sites that I know to be banned by the school;
- I will only e-mail people I know, or a responsible adult has approved;
- The messages I send, or information I upload, will always be polite and sensible;
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it;
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me;
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signature: _____ **Date:**_____

Full name (printed): _____

Appendix D: 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:	This risk or harm is covered in the following curriculum area(s):

	• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• Relationships education • Health education • RSE • Computing curriculum
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 • 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:	This risk or harm is covered in the following curriculum area(s):

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

	• How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	• 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 • 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	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• 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	• 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: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines). Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police	This risk or harm is covered in the following curriculum area(s): • Relationships education

	At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	
Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum area(s): • Relationships education
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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum

	• What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): • Health education
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum area(s): • Health education

Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): • Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): • RSE
Suicide, 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.	