Wessex Gardens Primary & Nursery School

Online Safety Policy

2021 - 2022

Growing Together

Wessex Gardens Primary and Nursery School is a place where we grow kind, confident, resilient and independent lifelong learners in a trusting and honest environment. Here everyone is welcome and valued. We are motivated and supported to reach our full potential as we continue to aspire to excellence.

Wessex Gardens Primary & Nursery School is committed to safeguarding and promoting the welfare of children in our care, and we expect all staff, governors, placements and volunteers to share this firm commitment.

This policy will be considered by the Governing Body on 30th March 2021

Approved by:	**Alexander Banks**	**Jill Summers**
Designation:	**Headteacher**	**Chairman of the Governing Body**
Signed:		
Date:	**30th March 2021**	**Review due by: July 2022**

Contents:

Statement of intent

Wessex Gardens Primary & Nursery 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, and there are a number of controls in place to ensure the safety of children and staff.

The breadth of issues classified within online safety is considerable, 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 children 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 children and staff.

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:

- Child Protection Policy
- Anti-Bullying Policy
- Safer Recruitment Policy
- Staff Professional Code of Conduct
- Behaviour Policy
- Safeguarding Policy
- Remote Learning Policy
- Complaints Policy
- Anti-Fraud Policy
- Photograph and Video 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.
- 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 children can develop an appropriate understanding of online safety.

- Organising engagement with parents/carers to keep them up-to-date with current online safety issues and how the school is keeping children safe.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Working with the DSL, ICT leader and IT consultants to conduct light-touch reviews of this policy.
- Working with the DSL, ICT leader and governing body to update this policy on a regular 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.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SLT, assistant SENDCO, ICT leader and IT consultants.
- 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 children 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 body about online safety.
- Working with the headteacher and ICT leader to conduct reviews of this policy.
- Working with the headteacher and governing body to update this policy regularly.

2.4. IT Consultants 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, headteacher and ICT leader to conduct 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. Children are responsible for:

- Adhering to this policy, the Pupil Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

3. The curriculum

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

- RSE
- PSHE
- 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. Children 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 children's ages and developmental stages.

3.5. The underpinning knowledge and behaviours children 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 risks children may face online are always considered when developing the curriculum.

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

3.8. The school recognises that, while any child can be vulnerable online, there are some children who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. children with SEND. Relevant members of staff, e.g. the assistant SENDCO and designated teachers and support staff, work together to ensure the curriculum is tailored so these children 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 children. 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 children?
- Are they appropriate for children's 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, DSL and ICT leader 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 children 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 child 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 child 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 children feel comfortable to say what they feel.

3.14. If a staff member is concerned about anything children raise during online safety lessons and activities, they will write a report in line with sections 15 and 16 of this policy.

3.15. If a child 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 15 and 16 of this policy.

4. Staff training

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

4.2. Online safety training for staff is updated annually and is delivered in line with advice from the LA and 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 Senior Leadership Team (SLT) 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 children safe while they are online at school.
- Recognise the additional risks that children with SEND face online and offer them support to stay safe online.

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

4.7. Staff are required to adhere to the Professional Code of Conduct at all times, 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 concerns.

5. Educating parents/carers

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

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

- Consultation evenings
- Training sessions
- Newsletters
- Messages and letters
- Encouraging signing up to National Online Safety https://nationalonlinesafety.com/

5.3. Parents/carers 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.

6. Classroom use

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

- Computers
- Laptops
- Tablets/IPads
- Intranet and Internet
- Cameras

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children use these platforms at home, the class teacher always reviews and evaluates the resource.

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

6.4. Children are supervised when using online materials.

7. Internet access

7.1. Children, staff and other members of the school community are only granted access to the school's internet network in line with the relevant Acceptable Use Agreement.

7.2. All members of the school community use the school's internet network, as it has the appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

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

8.2. The LGFL filtering and monitoring systems the school implements are appropriate for the age of the children.

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

8.4. The IT Consultant undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.5. The headteacher is notified by the IT consultant when changes are required to the filtering system.

8.6. Prior to making any significant changes to the filtering system, the headteacher, IT leader and DSL review the changes.

8.7. Any changes made to the system are recorded by the IT consultant.

8.8. Reports of inappropriate websites or materials are made to IT consultant immediately, who investigates the matter and makes any necessary changes.

8.9. Deliberate breaches of the filtering system are reported to the DSL, headteacher and IT leader, who will escalate the matter appropriately.

8.10. If a child has deliberately breached the filtering system, it will be investigated in line with the Behaviour Policy.

8.11. If a member of staff has deliberately breached the filtering system, it will be investigated in line with the Code of Professional Conduct and LA's Disciplinary Policy and Procedures.

8.12. If any illegal material is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. CEOP and/or the police.

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

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

8.15. Concerns identified through monitoring are reported to the headteacher and DSL who manages the situation in line with sections 15 and 16 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 IT Consultant.

9.2. Firewalls are switched on at all times.

9.3. The IT consultant reviews the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

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

9.5. Staff members and children report all malware and virus attacks to the ICT leader and IT consultant.

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

9.7. Children are provided with their own unique username and passwords for online learning platforms such as Google Classroom and Office 365.

9.8. Staff members and children are responsible for keeping their passwords private.

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

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

9.11. The IT consultant will reset usernames and passwords as required.

9.12. 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.

10. Emails

10.1. Access to, and the use of school emails, is managed in line with the Staff Acceptable Use Agreement.

10.2. Staff are given approved school email accounts, and they must use this account for school-related work.

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

10.4. Personal email accounts are not permitted to be used for school business.

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

10.6. Members of staff are required to block spam and junk mail, and report concerns to the IT leader.

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

10.8. Staff are advised that chain letters, spam and all other emails from unknown sources should be deleted without being opened.

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

11. Social networking

Personal use

11.1. Access to social networking sites on school premises is filtered as appropriate.

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

11.3. Staff are able to use personal social media during break and lunchtimes.

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 receive annual online safety training to help them use social media safely and responsibly.

11.6. Staff are not permitted to communicate with children or parents/carers over personal social networking sites, and are reminded to alter their privacy settings to ensure children and parents/carers are not able to contact them on social media.

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

11.8. 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, Professional Code of Conduct and Behaviour Policy.

Use on behalf of the school.

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

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

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

11.12. The Professional Code of Conduct contains information on the acceptable use of social media. Staff 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, and 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 children is not published on the website.

12.4. Images and videos are only posted on the website in line with the Photography and Video Policy and Images and Videos Parent/Carer Consent Form.

13. Use of school-owned devices

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

- Laptop/Tablet
- Mobile Phone

13.2. Children are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons and laptops/Chromebooks/iPads for remote learning.

13.3. School-owned devices are loaned to staff in accordance with the school's Loan Agreement.

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

13.5. All school-owned devices are password 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. The IT consultant reviews all school-owned devices to carry out software updates annually, and to ensure there is no inappropriate material on the devices.

13.8. No software, apps or other programs can be downloaded onto a device without authorisation from the ICT leader.

13.9. Staff members or children found to be misusing school-owned devices will be investigated in line with the Disciplinary Policy and Procedures, Behaviour Policy and Staff/Pupil Acceptable Use Agreement.

14. Use of personal devices

14.1. Staff personal devices are used in accordance with the Professional Code of Conduct.

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

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

- Toilets
- Cloakrooms
- Changing rooms
- Classrooms
- Corridors
- ICT room
- Library
- Work rooms

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

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

14.6. Staff members report concerns about their colleagues' use of personal devices on the school premises to the headteacher.

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.

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

14.9. If a child needs to contact their parents/carers during the school day, they can do so through the school office.

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

14.11. Children's devices can be searched, screened and confiscated in accordance with the DfE guidance 'Searching, screening and confiscation: advice for schools.'

14.12. If a staff member reasonably believes a child'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.

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

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

15. Managing reports of online safety incidents

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

- Staff training
- Staff briefings
- The online safety curriculum
- Assemblies
- Regular email updates

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. Professional Code of Conduct, LA's Staff Conduct Policy and the LA's Disciplinary Procedures.

15.3. Concerns regarding a child's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher, ICT leader, class teachers and IT Consultant.

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

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

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

15.7. Section 16 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 children 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 and Child Protection Policies.

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 Child Protection, Safeguarding and Anti-Bullying Policies.

16.7. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the 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, this may include police involvement, in line with the 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.
Following a report of sexting, the school follows the recommendation by the UK Council for Child Internet Safety's (UKCCIS) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people' guidance:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the children involved, if appropriate
- Parents/carers are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents/carers would put the child at risk of harm
- At any point in the process if there is a concern a child 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, children and their parents/carers are used to inform the action to be taken and the support to be implemented

16.15. Staff members do not view the youth produced sexual imagery.

16.16. When investigating a report, the DSL does not view the child produced imagery unless it is necessary in order to safeguard the child. This decision is based on the professional judgement of the DSL, following discussion with the headteacher, in line with the Child Protection Policy. In most cases the imagery will not be viewed.

16.17. Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

16.18. If it is necessary to view the imagery, it will not be copied, printed or shared.

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

Online abuse and exploitation

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

16.21. 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.

16.22. 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 Policy.

Online hate

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

16.24. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved

Online radicalisation and extremism

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

16.26. Concerns regarding a staff member or child being radicalised online are dealt with in line with the Child Protection Policy (includes 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 children 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.

17.3. All staff and children 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 some circumstances, e.g. to provide support for children with SEND. This will be decided and approved by the SLT.

17.5. Children not using devices or software as intended will be investigated in line with the Behaviour 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/carers prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternative 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, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

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

- Reinforce the importance of children staying safe online.
- Ensure parents/carers 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 controls on devices and internet filters to block malicious websites.
- Direct parents/carers to useful resources to help them keep their children safe online.

17.10. 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, headteacher, ICT leader and IT consultant conduct regular reviews of this policy to evaluate its effectiveness.

18.2. The governing body, headteacher, DSL and ICT leader review this policy in full on an annual basis and following any online safety incidents.

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