MOSELEY
CHURCH OF ENGLAND
PRIMARY SCHOOL

Online Safety Policy

(October 2020)

Signed by:

Headteacher Date:

Chair of governors Date:

Contents:

Appendices

Mission Statement

Our successful Christian school offers a wide range of exciting and educational opportunities to enhance skills, talents and creativity. The school community appreciates and accepts others, and celebrates the achievements of all. We have supportive and trusting relationships with God and all his children. As a result, we take responsibility and welcome absolutely everyone into a caring and safe environment, where we are all guided to work together.

School Aims

At Moseley C of E Primary School, we want ALL of our children to:

- Have an enthusiasm and thirst for learning
- Have confidence to be themselves and consistently aim high to challenge their potential;
- Have an awareness for the world beyond their own – have respect and understanding of others with circumstances different to their own;
- Explore all opportunities provided to discover their talents and abilities;
- To be kind and respectful members of their community;
- Have embedded morals;
- Have fun, good memories of their school life;
- Be inspirational role models.

Statement of intent

Moseley CofE 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.

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:

- Acceptable Use Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Remote Learning Policy

2. Roles and responsibilities

2.1. The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction and up to date refresher training at least annually.
- 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 at least annually.
- 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, Computing Lead and ICT technicians to conduct termly informal reviews of this policy.
- Working with the DSL, Computing Lead and governing board to update this policy on an annual basis.

2.3. The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, Computing Lead and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.

- Staying up-to-date with current research, legislation and online trends.
- Liaising with the school's Computing Lead to coordinate the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher, computing lead and ICT technicians to conduct termly informal reviews of this policy.
- Working with the headteacher, Computing Lead and governing board to update this policy on an annual basis.

2.4. ICT technicians are responsible for:

- Providing technical support for the 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, if required, to conduct reviews of this policy.

2.5. Computing Leader is responsible for:

- Ensuring that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Working with the headteacher, DSL and ICT technicians to conduct termly informal reviews of this policy.
- Working with the headteacher, DSL and governing board to update this policy on an annual basis.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, DSL and ICT technicians.

- Providing updated information to teaching staff to support teaching of online safety across the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Planning, resourcing and leading information sessions, newsletters, assemblies etc to inform parents and children about online safety issues as required.
- Ensuring online safety is considered in the school's approach to remote learning.

2.6. 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.

2.7. Pupils are responsible for:

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

3. The curriculum

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

- 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. 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 1 of this policy.

3.7. The DSL, the Computing Lead and the PSHE Lead are involved with the development of the school's online safety curriculum.

3.8. The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

3.9. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

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

3.11. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

3.12. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

3.13. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and 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 and in line with the Safeguarding and Child Protection 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 15 and 16 of this policy and in line with the Safeguarding and Child Protection 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 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 any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

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 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 Staff 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.

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:

- Parents' meetings.
- Letters to parents and carers
- Links and information on our school website

5.3. Parents are given a copy of the Acceptable Use Agreement when their child is admitted to our school and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.

6. Classroom use

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

- Computers
- Laptops
- iPads
- Cameras
- Dictaphone

- Web-cams

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 must use the school’s internet network, 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 board ensures the school’s ICT network has appropriate filters and monitoring systems in place.

8.2. The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. Our school uses the Smoothwall filtering system.

8.3. The filtering and monitoring systems the school implements are appropriate to pupils’ ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

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

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

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

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

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

8.9. Reports of inappropriate websites or materials are made to the DSL immediately, who will liaise with the computing lead an ICT technician to investigate the matter and make any necessary changes.

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

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

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

8.13. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. Action can also be taken in line with the Computer Misuse Act.

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

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

8.16. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 15 and 16 of this policy and the Safeguarding and Child Protection Policy.

9. Network security

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

9.2. Firewalls are switched on at all times.

9.3. ICT technicians 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 advised not to download unapproved software or open unfamiliar email attachments.

9.5. Staff members and pupils report all malware and virus attacks to the headteacher or School Business Manager or Computing Lead who will inform ICT technicians.

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

9.7. Pupils are provided with their own unique username and private passwords.

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

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

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

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

9.12. Users inform ICT technicians if they forget their login details, who will arrange for log in details to be reset.

9.13. 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.

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

10. Emails

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

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 is only sent using secure and encrypted email.

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

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

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

10.9. The computing lead organises at least one annual assembly for KS2 children focussed on online safety which will include an explanation of what a phishing email and other malicious emails might look like – this assembly includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email (this will be taught to children in an age appropriate way.)

10.10. 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. Pupils are not allowed on Social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

11.2. In the event that a pupil or parents uses social networking sites to make inappropriate comments about the school or school staff advice will be sought from relevant agencies, including the police, and appropriate action will be taken if necessary.

11.3. Staff and pupils are not permitted to use social media for personal use during lesson time.

11.4. Staff must not access social networking sites using school equipment.

11.5. Staff must not reveal names of staff, pupils, parents/carers or any other member of the school community or discuss school related matters on any social networking site or blog.

12. Use of Social Media

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

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

12.3. 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.

12.4. Pupils in KS2 are taught how to use social media safely and responsibly through the online safety curriculum.

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

Use on behalf of the school

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

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

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

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

12.10. 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.

13. The school website

13.1. 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.

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

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

13.4. The school record of parental permissions granted / not granted must be adhered to when taking images of our children. Permissions are recorded on a central list which is kept in the school office with the parental contact forms. Images and videos are only posted on our school website when parental permission has been granted.

14. Use of school-owned devices

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

- Laptop
- Web cam
- iPad

14.2. Pupils may be provided with school-owned devices as necessary to assist in the delivery of the curriculum in lessons e.g. iPads to use during lessons.

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

14.4. Staff who are provided with school owned devices are required to read, sign and uphold the Staff Device User Agreement.

14.5. Pupils who are provided with school owned devices are required to read, sign and uphold the Pupil Device User Agreement.

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

14.7. All school-owned devices are password protected and have bitlocker encryption enabled.

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

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

14.10. Staff members must not use school owned equipment for personal use.

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

15. Use of personal devices

15.1. Staff members are not permitted to use their personal devices during lesson time or in spaces that are accessible to children.

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

15.3. Staff members should report any concerns about their colleagues' use of personal devices on the school premises in line with the Safeguarding and Child Protection Policy or Whistleblowing Policy.

15.4. 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 Safeguarding and Child Protection Policy.

15.5. Pupils are not permitted to use their personal devices anywhere on the school site. Any personal electronic device including mobile phones brought into school by a pupil must be stored securely in the school office.

15.6. If a pupil needs to contact their parents during the school day, they should discuss this with their class teacher.

15.7. Pupils' personal devices can be confiscated and stored securely. The headteacher will contact the pupils parent / carer to discuss the reasons for the item being confiscated and arrange for the device to be collected by the parent / carer.

15.8. 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 confiscated and handed to the police.

15.9. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Visitors will be provided with advice about appropriate use of personal devices when on the school site.

15.10. Parents and carers attending events at the school will be advised about appropriate use of personal devices when on school site.

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

16. Managing reports of online safety incidents

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

- Staff training
- The online safety curriculum
- Assemblies

16.2. 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, including the Staff Code of Conduct and Safeguarding and Child Protection Policy.

16.3. Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians.

16.4. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, including the Behaviour Policy and Child Protection and Safeguarding Policy.

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

16.6. All online safety incidents should be reported to the DSL and the school's response will be recorded by the DSL.

16.7. Section 16 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

17. Responding to specific online safety concerns

Cyberbullying

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

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

17.3. 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)

17.4. 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

17.5. 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.

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

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

Upskirting

17.8. 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.

17.9. 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.

17.10. “Operating equipment” includes enabling, or securing, activation by another person without that person’s knowledge, e.g. a motion activated camera.

17.11. Upskirting is not tolerated by the school.

17.12. Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

17.13. 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.

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

17.15. 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

17.16. 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.

17.17. 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.

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

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

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

17.21. Viewing and deleting imagery will be carried out in line following advice from other agencies including police and children's social care.

Online abuse and exploitation

17.22. 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.

17.23. 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.

17.24. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

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

17.26. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy, Parent and Visitor Code of Conduct and Social Media Code of Conduct for Parents.

Online radicalisation and extremism

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

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

18. Remote learning

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

18.2. Parents are responsible for maintaining supervision of their child whilst they are learning remotely.

18.3. All staff and pupils using video communication must:

- Only communicate in groups.
- 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.
- Endeavour to ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

18.4. 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.
- Endeavour to ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

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

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

18.7. 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.

18.8. The school will endeavour to consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable.

School will endeavour to make suitable alternative arrangements where necessary.

18.9. 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.

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

18.11. During the period of remote learning, the school will provide information for 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.
- 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.

18.12. 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.

19. Monitoring and review

19.1. The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct termly informal reviews of this policy to evaluate its effectiveness.

19.2. The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

19.3. The next scheduled review date for this policy is October 2021

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

Appendix 1: Online harms and risks – curriculum coverage

[The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.]

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum area(s): • PSHE • Computing curriculum
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): • PSHE • 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	• PSHE • 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): • PSHE • 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): • PSHE • 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): • PSHE • 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): • PSHE • Computing curriculum
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms	This risk or harm is covered in the following curriculum area(s): • PSHE

	- That privacy settings have limitations	- 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): - PSHE - 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): - PSHE - Computing
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: - What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal - How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why	This risk or harm is covered in the following curriculum area(s): - PSHE

	• 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	
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): • PSHE
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): • PSHE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum area(s): • PSHE • Computing curriculum

Wellbeing		
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): • PSHE
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): • PSHE
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.	

MOSELEY CHURCH OF ENGLAND PRIMARY SCHOOL

Child-friendly technology acceptable use agreement

At Moseley CofE Primary School, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.

I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- ✗ Tell another pupil my username and password.
- ✗ Share personal information, such as my age and where I live, about myself or my friends online.
- ✗ Access social media, such as Facebook and WhatsApp.
- ✗ Speak to strangers on the internet.
- ✗ Take photos of myself or my friends using a school device.

Please read each statement and provide a tick to show that you agree, and then write your name below.

✓

- □ I understand why it is important to use technology safely and correctly.
- □ I understand my responsibilities when using technology.
- □ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- □ I will follow these rules at all times.

Pupil name (please print): ______________________________

Date: ______________________________

Parent name (please print): ______________________________

Parent signature: ______________________________

Date: ______________________________

Devices user agreement – staff

This agreement is between Moseley CofE Primary School and ________________________________and is valid the duration of their employment at the school.

Moseley CofE Primary School has created this agreement to ensure that all staff understand their responsibilities when using school-owned devices, such as mobile phones and tablets, whether on or off the school premises.

Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school

Moseley CofE Primary School retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

Under this agreement, the school will:

- Provide devices for your sole use while you are a permanent full-time or part-time teacher at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the relevant persons, such as the ICT technicians, have installed the necessary security measures on any school-owned device before your use – including, but not limited to, the following:
  - Firewalls
  - Malware protection
  - User privileges
  - Filtering systems
  - Password protection and encryption
  - Mail security technology
  - Tracking technology
- Ensure that all devices undergo the following regular checks and updates by the ICT technicians in line with school policy:
  - updates to malware protection
  - software updates
  - password re-set requirements
  - checks to detect any unchanged default passwords
  - Malware scans in line with specific requirements
- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.
- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

Under this agreement, you will:

Overall use and care

- Bring the device and charging unit to the school each day and keep the device with you, or store it securely at all times.
- Transport the device safely.
- Not permit any other individual to use the device without your supervision, unless agreed by the headteacher.
- Take responsibility for any other individual using the device.
- Provide suitable care for the device at all times and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Ensure all devices are switched off when not in use.
- Immediately report any damage or loss of the device to the headteacher.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the headteacher or school business manager
- Be prepared to cover the insurance excess, repair or replacement of the device when the damage or loss has been a result of your own negligence.
- Make arrangements for the return of the device and passcode to the headteacher or school business manager if your employment ends or if you will be away from the school for more than two weeks.

Using devices

- Only use the devices that have been permitted for your use by the headteacher.
- Only use devices for school purposes.
- Only use apps or programmes that are GDPR-compliant and from reputable sources.
- Ensure that any personal data is stored in line with the GDPR.
- Only store sensitive personal data on your device where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device is encrypted.
- Give permission for the ICT technicians to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the headteacher.
- Not install any software onto your device unless instructed to do so by the ICT technician or headteacher.
- Ensure your device is protected by anti-virus software installed by the ICT technician and that this is checked on a regular basis.
- Not use your device to take images or videos of pupils, staff or parents unless permission has been granted by parents and carers in line with the school's Image and Video Parental Consent Form.
- In line with the above, only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- Not use your device to communicate with pupils or parents, other than using platforms permitted by the headteacher.

- Not use your device to send any inappropriate messages, images or recordings.
- Ensure that your device does not contain inappropriate or illegal content.
- Only access social media sites for school purposes that have been approved by the headteacher on your device, and ensure they are used in accordance with the Acceptable Use Agreement.
- Allow the ICT technicians to monitor your usage of your device, such as internet access, and understand the consequences if you breach the terms of this agreement.

Insurance cover provides protection from the standard risks whilst the device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave the device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

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

Signed: Date:

Print name: Device model and number:

Headteacher:

Signed: Date:

Print name:

Devices user agreement – Pupils

This agreement is between Moseley CofE Primary School ___________________________________

and is valid between_____________________________and _________________________________.

The device is the property of the school and must be returned to school for monitoring when requested..

We have created this agreement to make sure you understand how devices must be used. If you do not follow this agreement, appropriate action will be taken by the school and you may have your device taken off you.

General use principles

- The device belongs to the school and is given on loan to you.
- The device should be brought to school fully charged every day if you are attending school.
- The device should be kept with you in your classroom or handed to your teacher so that it can be stored safely.
- The device should be taken home with you at the end of the day or returned to your class teacher who will store it safely.
- You should never leave the device unattended. Unattended devices will be collected and stored in the school office.
- If you leave the school before completing the school year, you must return the device to your teacher.
- If the device is damaged, lost or stolen you must report it to a staff member immediately.
- If you think the device has been stolen, you must report it to the police and tell a staff member.
- If you lose or damage any covers, chargers or other equipment for the device, you must replace it.
- If you damage or lose the device, you must pay for a replacement or repair costs.
- You must not use your device around food or drink.

The school will:

- Make sure the device is secure and has password-protection.
- Monitor your usage of the device to make sure it is being used correctly.
- Make sure all data is backed up securely and remove data every year.

You will:

- Use all devices appropriately and responsibly.
- Only use your device for educational purposes.
- Not play any games on the device during the school day other than those used in lessons for educational purposes.
- Make sure sounds are muted and not play any music, unless the teacher gives you permission to do so.
- Store devices safely.
- Obey school rules for behaviour and communication on devices.
- Follow this agreement and take care of devices.
- Follow any instructions from staff.
- Give the device back to your teacher at the end of the school year.
- Use any electronic communication appropriately.
- Only access the school’s Wi-Fi with permission from your teacher.

You will not:

- Modify the device in any way, unless a staff member has given you permission to do so.
- Apply marks, stickers or other decorations to the device.
- Give devices to other pupils.
- Remove any covers from the device.
- Sync the device with any computer.
- Delete browsing history from the device.
- Disable any applications on the device, such as tracking.
- Access any websites that you have not been given permission to do so.
- Send any inappropriate messages.
- Send, access or upload any inappropriate images and videos.
- Access any other pupil's account or files on the device.

Please read each statement and provide a tick to show you agree to the terms, then provide your name below.

- I will use my device appropriately.
- I will follow this agreement at all times.
- I understand that if I do not follow this agreement my device may be taken off me and there may be other disciplinary actions.

Pupil name (please print): ____________________________________
Date: ____________________________________

Parent name (please print): ____________________________________
Parent signature: ____________________________________
Date: ____________________________________

Borrowing IT Equipment Agreement - Parents

This agreement is between Moseley CofE Primary School and the parents and carers of ____ who are borrowing school IT equipment, and is valid from _______________ to ____________________. The device is the property of the school and activity can be monitored for any breaches of the school's Technology Acceptable Use Agreement.

We have created this agreement to ensure you understand your responsibilities as a parent whilst your child is borrowing IT equipment from the school.

Responsibilities

- You must ensure your child treats the device in line with the school's Technology Acceptable Use Agreement – the school has provided parents with this via the school website.
- You must ensure that the device is not used for any personal reasons by your child
- You must ensure nobody but your child has access to the device.
- You must ensure the device is stored safely.
- You must make sure the device is not used near any food or drink.
- If you remove your child from the school before completing the school year or during the agreed loan period, you must return the device to the school.
- If your child is excluded from the school, you must return the device to school.
- If the device is lost stolen, you must report it to the school and the police immediately.
- If the device is damaged, you must report it to the school immediately.
- If covers, chargers or other equipment for the device are damaged whilst it is in your child's possession, you must pay for a replacement or repair costs.
- If the device is damaged whilst it is in your child's possession, you must pay for the replacement or repair costs.
- You must ensure your child understands their responsibilities for looking after the device, as outlined in the school's Device User Agreement – Pupils – this must be signed and returned before the school releases any IT equipment on loan.
- You must ensure any software damage, e.g., viruses are reported to the school immediately.
- You must ensure that no applications are disabled on the device and make sure the device is not modified in any way or synced with another device.
- You and your child must have due regard to the school's Loaning School Equipment Policy.

Please read each statement and provide a tick to show you agree to the terms, then provide your name below.
This must be returned to ______________________________________ via the school office.

- □ I will carry out my responsibilities as outlined in this agreement.
- □ I will ensure my child has read and signed the **Device User Agreement - Pupils**.
- □ I understand that I must pay for any loss or damage to either the device or any equipment for the device.

Parent name (please print): ____________________________________
Parent signature: ____________________________________
Date: ____________________________________