Online Safety Policy

Author:	Noelle Sturla
Date of approval:	March 2022
Next review date:	March 2025
Review period:	3 years
Status:	Recommended

1. Compliance

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

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

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement (Staff and Students: Appendices A and B)
- Safeguarding Policy
- Anti-Bullying Policy
- Relationships and Sex Education (RSE) and Health Policy
- Code of Conduct for all Adults (working with children at Farmor's School)
- Behaviour Policy
- Data Protection Policy
- Confidentiality Policy

2. Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the remit of the Designated Safeguarding Lead (DSL) covers online safety.
- Reviewing this policy on a 3 yearly cycle.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

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 and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct light-touch annual reviews of this policy.

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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's safeguarding reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

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

3. Managing online safety

3.1.   Technology is a significant component in many safeguarding and wellbeing issues affecting young people.

3.2.   The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

3.3.   The importance of online safety is integrated across all school operations in the following ways:
- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum

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

3.5   Concerns regarding a staff member's online behaviour should be reported to the headteacher, who will decide on the best course of action in line with the relevant policies, e.g. the Code of Conduct (Adults), Allegations of Abuse Against Staff Policy, and Conduct Policy. If the concern is about the headteacher, it is reported to the chair of governors.

3.6   Concerns regarding a pupil's online behaviour should be reported to the DSL, who will investigate concerns with relevant staff members, e.g. the headteacher and ICT technicians, and will manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Safeguarding Policy.

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

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

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

4. Cyberbullying

4.1 Cyberbullying can include the following:
- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

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

5. Peer-on-peer sexual abuse and harassment

5.1. Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

5.2. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:
- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

5.3. Staff should be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the

imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

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

6. Grooming and exploitation

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

6.2. Staff should be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:
- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

6.3. Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming in a pupil are, including:
- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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

6.4. Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online

to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

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

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

Radicalisation

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

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

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

7. Mental health

7.1. The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

7.2. Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

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

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

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

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

8.5. Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:
- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Safeguarding Policy.

8.6. Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

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

9. Cyber-crime

9.1. Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:
- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

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

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

9.3. The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Online safety training for staff

10.1 The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including information as to how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

10.2 Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Safeguarding Policy.

11. Online safety and the curriculum

11.1 Online safety is embedded throughout the curriculum; however, it is particularly addressed in PSHE, IT and the Assembly Programme.

11.2 Online safety teaching is always appropriate to pupils' ages and developmental stages.

11.3 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. 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
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts

- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

11.4 The online risks pupils may face online should always be considered when developing the curriculum.

11.5 The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

11.6 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.

11.7 The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

11.8 Class teachers should review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for their cohort of pupils. When reviewing these resources, the following questions should be 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?

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

11.10 Before conducting a lesson or activity on online safety, the class teacher will 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 will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities should be 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.

11.11 During an online safety lesson or activity, the class teacher should ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

11.12   If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding Policy.

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

12.   Use of technology in the classroom

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

- Computers
- Laptops
- Email
- Cameras
- Mobile phones

12.2   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 should review and evaluate the resource. Class teachers should ensure that any internet-derived materials are used in line with copyright law.

12.3   Pupils should be supervised when using online materials during lesson time – this supervision should be suitable to their age and ability.

13.   Use of smart technology

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

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

13.3   Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Agreement.

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

13.5   Inappropriate use of smart technology may include:

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

13.6   Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom, without explicit permission given by the teacher.

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

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

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

14. Educating parents

14.1 The school will continue to work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement when their child is admitted and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

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

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

14.4 Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources

15. Internet access

15.1 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.

15.2 All members of the school community are encouraged to use the school's internet network where practical and permitted, instead of 3G, 4G and 5G networks, as the school network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

16.1   The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

16.2   The headteacher and ICT technicians will undertake regular risk assessments to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians should undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

16.3   Requests regarding making changes to the filtering system are directed to the DSL. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technician, who will investigate the matter and make any necessary changes.

16.4   Deliberate breaches of the filtering system should be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Conduct Policy.

16.5   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.

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

17. Network security

17.1   Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times and are managed by an external provider (Exa). Any changes required need to be actioned by this provider.

17.2   Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

17.3   All members of staff have their own unique usernames and private passwords to access the school's systems. All pupils are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Staff passwords require a two-factor authentication.

17.4 Users should inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a staff user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take. If a pupil user is found to be doing the same, the school behaviour policy is followed.

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

18. Emails

18.1 Staff and pupils are given approved school email accounts should only use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

18.2 Staff members and pupils are required to block spam and junk mail, and raise any concerns to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

19. Social networking

Personal use

19.1 Access to social networking sites via the school network is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

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

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

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

Use on behalf of the school

19.5 The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

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

20. The school website

20.1 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.

20.2 The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if permission is granted by the headteacher.

21. Use of devices

School-owned devices

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

- Laptop
- Mobile phone (from the school pool for trips/fixtures/safeguarding)

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

21.3 School-owned devices should be used in accordance with the Laptop Protocol. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected.

21.4 ICT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. Staff are permitted to install software, apps or other programmes required for their teaching.

Personal devices

21.5 Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

21.6   Staff members should report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

21.7   Pupils in the lower school (Y7-11) are not permitted to use their personal devices during lesson time (unless given permission by the subject teacher) or on the school site. If a pupil needs to contact their parents during the school day, they are allowed to use the telephone in student services. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use. Students in the 6th form are permitted to use personal devices.

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

21.9   Pupils' devices can be searched, screened and confiscated in accordance with the Behaviour Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

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

22.   Remote learning

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

22.2   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.

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

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

22.4   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.

23.   Monitoring and review

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

23.2   The governing board, headteacher and DSL will review this policy in full on a three year basis and following any online safety incidents.

23.3   Any changes made to this policy will be communicated to all members of the school community.

7. ACCEPTABLE USE POLICY (Staff)

ICT Acceptable Use Policy

Farmor's School is committed to providing ICT facilities (including internet, email and Office 365) to employees and to promoting employee awareness of the benefits and dangers involved. Improper use of the internet or email could bring the school into disrepute and may lead to legal claims against individuals and the school. Infringement of this policy by employees may be regarded as a disciplinary offence and in serious cases, may result in dismissal.

A copy of this policy is displayed around the school and is available on SharePoint.

Computer network

Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, discriminatory, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will lead to disciplinary action.

Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.

You are responsible for the security of your passwords.
The network must not be used for commercial purposes, e.g. buying or selling goods.
The installation of software on the network must only be done with the approval of the Network Manager.
Any software that is installed must be covered by the appropriate licensing agreements.
Copyright of materials available on the network must be respected.

Internet / Email

Use of the Internet and email must be solely for educational purposes.
Use of the internet and email are subject to scrutiny by the school. Any action that might damage the good reputation of the school will be dealt with as a serious act of misconduct and will lead to disciplinary action.
Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
Emails sent from the school account should contain the same professional levels of language and content as applied to letters or other media.
You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received.
Posting anonymous messages and forwarding chain letters is forbidden.
Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email.

If you are in any doubt about any of the above, please seek advice.

ACCEPTABLE USE POLICY (Pupils)

ICT Acceptable Use Policy

Farmor's School is committed to providing ICT facilities (including internet, email and Office
365) to pupils and to promoting pupil awareness of the benefits and dangers involved.
Infringement by pupils may result in the withdrawal of access to hardware or software
and in serious cases (particularly those that break the law) pupils may be excluded and
referred to the police. Improper use of the internet or email could bring the school into
disrepute and may lead to legal claims against individuals and the school.

Computer network

You must not install, or attempt to install, programs of any type on a machine, or store
programs on the computers or network, without permission.
You must not damage, disable or otherwise harm the operation of computers, or
intentionally waste ICT resources.
You will not use the network for commercial purposes, e.g. buying or selling
goods. You must not disclose your password or use passwords intended for the
use of others. You must not use the network in a way that may harass, harm,
offend or insult others.
You are expected to respect and not attempt to bypass security in place on the network.
You must not access, copy, remove or otherwise alter other people's work, or attempt
to alter the settings on the computers.
You may not plug any personal device into the mains power, or into any school device
e.g. via USB, either to use it or to charge it.

Internet / Email

You may access the internet only for study purposes or school authorised activities.
You must not use the internet to obtain, download, send, print, display or otherwise
transmit or gain access to materials which are unlawful, obscene or abusive.
You are expected to respect the work and ownership rights of people outside school as
well as pupils and staff. This includes abiding by copyright laws.
You must not engage in chat activities over the internet whilst at school.
You should be aware that messaging services available outside of school are open
forums and subject to public scrutiny.
Any incidents of abuse, discriminatory or defamatory statements or anything that might
damage the good reputation of the school will be dealt with as serious acts of
misconduct.
You will not give personal information such as your address or telephone number to
those who you contact through use of the school's ICT systems.

Sanctions

Violations of these rules will result in the withdrawal of access to all ICT resources and a
letter will be sent home to your parents/ guardian explaining the reasons for withdrawal.
Additional action may be taken by the school. Serious violations will result in the police
being involved and / or other legal action take