Churnet View Middle School

Online Safety Policy

Last updated: September 2020

Contents:

Statement of intent

Churnet View Middle 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 Agreement
- Anti-Bullying Policy
- Behaviour Policy
- Home School Agreement
- TTLT Information Sharing Policy
- Safeguarding/Child Protection Policy

2. Roles and responsibilities

2.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority

2.2 The Governing Body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

2.3 The e-safety officer, Victoria Shepherd, is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

2.4 The e-safety officer is responsible for contributing agenda points to e-safety sections of the general Health and Safety meeting, which includes representatives of the school SLT, teaching staff, governors, parents, pupils and the wider school community.

2.5 The headteacher is responsible for ensuring that the DSL and/or DDSLs and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

2.6 The DSL and/or e-safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

2.7 The headteacher and data protection officer (DPO) will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

2.8 The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher and DSL, when appropriate, at the Health and Safety committee meeting.

2.9 The DSL and DDSLs will ensure that My Concern is used appropriately by staff for reporting incidents and inappropriate internet use, either by pupils or staff.

2.10 The DSL, DDSL and/or the e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

2.11 The DSL, DDSL and/or the e-safety officer officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

2.12 The Governing Body will hold regular meetings with the the DSL, DDSL and/or the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

2.13 The Governing Body will evaluate and review this E-safety Policy annually, to understand the latest developments in ICT and the feedback from staff/pupils.

2.14 The headteacher will review and amend this policy with the DSL, DDSL and/or the e-safety officer officer and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

2.15 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

2.16 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this Esafety Policy.

2.17 All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign when they log on to a PC. All staff and pupils will understand and adhere to the Acceptable Use Agreement which is available on the school website, and agreed to on initial introduction to the school.

2.18 Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. Additional learning is given to pupils via computer studies lessons.

2.19 The DSL, DDSL and/or the e-safety officer is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

2.20 All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

3. The curriculum

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

- RSE
- Health education
- RESPECT
- 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.

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

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

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

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

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

3.11. Before conducting a lesson or activity on online safety, the class teacher considers 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 report this to the DSL/DDSL using My Concern.

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.

4. Staff training

4.1. CPD to support staff on E-safety is available.

4.2. All staff will be provided with e-safety updates and training throughout the academic year to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

4.3. All staff will undergo at least one audit per academic year so that the DSL, DDSL and/or the e-safety officer officer is able to identify training needs.

4.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.5. All staff will be educated on which sites are deemed appropriate and inappropriate.

4.6. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.7. Any new staff are required to undergo e-safety training as a part of their induction programme, ensuring they fully understand the e-safety policy.

4.8. The e-safety officer will offer staff support when they require e-safety advice.

5. Educating parents

5.1. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media and family e-safety homework. Relevant presentations will also be made available for parents, when required.

5.2. Parents' evenings, meetings, telephone calls home and other similar occasions will be utilised to inform parents of any e-safety related concerns.

6. Classroom use

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

- Computers
- Laptops
- Tablets
- Internet
- Email

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

7. Internet access

7.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

7.2. Where a pupil is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify the parents that the pupil has consented independently.

7.3. A record will be kept by the headteacher of all pupils who have been granted internet access.

7.4. All users in KS2 and above will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

7.5. Ongoing reminders are issued to the pupils to ensure that they keep their passwords safe and confidential.

7.6. Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

7.7. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

7.8. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

7.9. The Governing Body will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

7.10. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.

7.11. All school systems will be protected by up-to-date virus software.

7.12. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

7.13. Master users' passwords will be available to the headteacher for regular monitoring of activity.

7.14. Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

7.15. Personal use will only be monitored by the DSL, DDSL and/or the e-safety officer officer for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

7.16. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

8. Filtering and monitoring online activity

8.1. The Health and Safety committee will evaluate and review this E-safety Policy frequently, taking into account the school's e-safety calendar, the latest developments in ICT and feedback from staff/pupils.

8.2. This policy will also be reviewed on an annual basis by the Governing Body; any changes made to this policy will be communicated to all members of staff.

8.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

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

8.5. Deliberate breaches of the filtering system are reported to the DSL, DDSL, e-safety officer and ICT technicians, who will escalate the matter appropriately.

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

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

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

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

8.10. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 15 and 16 of this policy.

9. Network security

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

9.2. Firewalls are switched on at all times.

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

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

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

9.6. Pupils in Year 5 and above are provided with their own unique username and private passwords.

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

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

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

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

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

9.12. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

10. Emails

10.1. Access to and the use of 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.

11. Social networking

Personal use

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

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

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

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

11.5. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

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

11.7. Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

Use on behalf of the school

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

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

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

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

11.12. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

12.1. The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

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

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

13. Use of school-owned devices

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

- iPad
- Pupil laptops (where necessary)

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

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

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

13.5. All school-owned devices are password protected.

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

13.7. Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Behavioural Policy.

14. Use of personal devices

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

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

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

- Toilets
- Changing rooms

14.4. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency, to contact the school office or a member of Senior Management.

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

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

14.7. If a pupil needs to contact their parents during the school day, they are allowed to request this via the school office.

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

14.9. Pupils' devices can be searched, screened and confiscated in accordance with the Behavioural Policy.

14.10. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

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

15. Managing reports of online safety incidents

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

- Staff training
- The online safety curriculum
- Assemblies

15.2. Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies.

15.3. 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.

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

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

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

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

16. Responding to specific online safety concerns

Cyberbullying

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

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

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

16.3. The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

16.4. The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

16.5. 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.

16.6. 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

16.7. Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

16.8. A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

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

16.10. Upskirting is not tolerated by the school.

16.11. 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)

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

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

16.14. 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

16.15. 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.

16.16. 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.

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

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

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

16.20. Viewing and deleting imagery is carried out in line with the behavioural policy.

Online abuse and exploitation

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

16.22. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

16.23. 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

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

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

Online radicalisation and extremism

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

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

17. Remote learning

17.1. All remote learning is delivered in line with the school's E-Safety policy – Section 17 Remote Learning

17.2. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

17.3. All staff and pupils using audio communication must:

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

- Always remain aware that they can be heard.

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

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

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

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

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

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

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

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

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

18. Monitoring and review

18.1. The school recognises that the online world is constantly changing; therefore, the e-safety officer, ICT technicians and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

18.2. The governing board, headteacher and e-safety officer review this policy in full on an annual basis and following any online safety incidents.

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