Enable Trust

On-Line Safety Policy

Our Vision

Achieving More Together

Our Mission

Working together passionately to achieve the best outcomes for our SEND children and young people

Ratified by:	Achievement, Support & Outreach Committee
Ratification Date:	07/03/2024
Review Frequency: *Annual, Bi-Annual* (Subject to Academy Trust or national policy change)	Annual
Review Date:	Sept'24
Related Policies:	See Section 3

Contents

Version Control

Version No.	Amendments	Date
V1.0	Trust-wide policy created, adopted by NSS	Jan’23
V1.1	Policy updated to be adopted by all schools	Feb’24

1 Policy aims

Enable Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning.

The aim of this policy is to ensure appropriate and safe use of the internet and other digital technology devices by all pupils, staff and other members of the school community.

The use of online services is embedded throughout our schools, therefore the Trust aims to:

- Have robust processes in place to ensure the online safety of all pupils, staff, volunteers and governors and trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The breadth of issues classified within online safety is considerable however the measures implemented to protect pupils and staff can be categorised into four 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.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2 Legislation and guidance

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

- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'OnLine Safety Act'
- DfE 'Meeting digital and technology standards in schools and colleges'
- The UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018
- National Cyber Security Centre - 'Cyber Security: Small & medium Organisations Guide'
- DfE (2023) 'Teaching online safety in school'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- 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 (2022) 'Searching, screening and confiscation'
- Voyeurism (Offences) Act 2019
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

3 Related policies

This policy operates in conjunction with the following Trust/School policies:

- Acceptable Use Agreement: staff, volunteers and pupils.
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Positive Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy

4 Roles and responsibilities

4.1 The Board of Trustees have oversight for this Trust policy but its implementation is delegated to the Local Governing Body (LGB) of each school.

4.2 The LGB is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring that there are appropriate filtering and monitoring systems in place to meet the DfE's "Filtering and monitoring standards for schools and colleges" and that reviews are undertaken at least annually.
- Ensure that the results of the online safety reviews are recorded for reference and made available to those entitled to inspect that information.

- Ensuring the Designated Safeguarding Lead (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.
- Ensuring that all relevant trust and school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

4.3 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 that staff understand this policy, and that it is being implemented consistently throughout the school/trust.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Supporting the DSL by ensuring there is enough time and resources to deal with all online safeguarding issues.
- Ensuring online safety practices are reviewed.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and Online Safety Lead to conduct annual reviews of this policy.
- Working with the DSL and governing board to recommend updates to this policy to the Board of Trustees on an annual basis.

4.4 The Online-Safety Lead is responsible for:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensuring filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Working with the DSL, ICT technician and a Governor to conduct annual reviews of online safety.
- Keep records of checks to the filtering provision as part of the filtering and monitoring review process.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Taking guidance from the DSL so that 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.
- Reporting to the governing board about online safety.
- Working with the DSL and Director of Finance & Operations (DFO) to update this policy on an annual basis.

4.5 Responsibilities of the IT Support Provider:

- Ensuring an appropriate level of security protection procedures are in place, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that School and Trust IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

4.6 All staff members are responsible for:

- Adhering to this policy, the Acceptable Use Agreement, and other relevant policies.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours including in their use of social media.
- 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.

4.7 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 have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

5 Educating pupils about online safety

5.1 Online safety is embedded throughout the curriculum however, it is particularly addressed in the PSHE, ICT and in Assemblies.

5.2 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, DfE's 'Teaching online safety in school' guidance, NSPCC and CEOP.

5.3 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.

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

5.5 The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- 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

5.6 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.

5.7 The Online Safety Lead is involved with the development of the school's online safety curriculum.

5.8 The Trust 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 CLA. Relevant members of staff, e.g. the SENDCO and designated teacher for CLA, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

5.9 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?

5.10 External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL agree invitations of external groups into school and ensure the visitors selected are appropriate.

5.11 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.

5.12 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.

5.13 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 asking questions and are not worried about getting into trouble or being judged.

5.14 If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with this policy.

5.15 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 16 and 17 of this policy.

6 Educating parents/carers about online safety

6.1 Our schools work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about their pupil's school approach to online safety and their role in protecting their children.

6.2 Parents of new pupils are sent a copy of the Acceptable Use Agreement on admission and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

- 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.

6.4 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.

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

- Via the School Websites
- Parents' evenings
- Newsletters
- Online resources
- Annual review meetings
- Personalised approaches specific to their child's needs

7 Staff Training

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

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

7.3 Online safety training for staff is updated annually and is delivered in line with advice from South Gloucestershire Safeguarding Training team.

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

7.5 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.

7.6 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.

7.7 Staff must adhere to the Trust's Staff Professional Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

7.8 All staff are informed about how to report online safety concerns, in line with this policy.

7.9 The **Online Safety Lead** in each School acts as the first point of contact for staff requiring advice about online safety.

8 Classroom Use

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

- Laptops
- Tablets/ipads
- Augmentative Alternative Communication devices (AACs)
- Email
- Cameras
- Audio recorders

8.2 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.

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

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

9 Internet Access

9.1 Use of the school/trust's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

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

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

10 Filtering and Monitoring Online Activity

10.1 The Director of Finance and Operations ensures the schools' ICT networks have appropriate filters and monitoring systems in place to meet the DfE's "Filtering and monitoring standards for school" guidance.

10.2 The Headteacher and IT Support technicians should undertake a risk assessment to determine what filtering and monitoring systems are required.

10.3 Filtering and monitoring provision is reviewed within each school, which can be part of a wider online safety review, at least annually.

10.4 The filtering and monitoring systems implemented 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.

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

10.6 The IT support provider undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

10.7 Requests regarding making changes to the filtering system are directed to the Headteacher

10.8 Prior to making any changes to the filtering system, the IT Support Provider and the Online Safety lead conduct a risk assessment.

10.9 Any changes made to the system are recorded by the IT Support Provider.

10.10 Reports of inappropriate websites or materials are made to the IT Support Provider immediately, who will investigate the matter and makes any necessary changes.

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

10.12 If a pupil has deliberately breached the filtering system, they will be disciplined

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

10.14 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.

10.15 The school/trust's networks and school-owned devices are appropriately monitored.

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

10.17 Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 18 and 19 of this policy.

11 Network Security

11.1 Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT Support Provider.

11.2 Firewalls are switched on at all times.

11.3 The IT support provider reviews the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

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

11.5 Staff members and pupils report all malware and virus attacks to the IT Support Provider

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

11.7 Pupils in class year or key stage and above are provided with their own unique username and private passwords.

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

11.9 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. Passwords expire after 90 days, after which users are required to change them.

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

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

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

9.14. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher or Director of Finance & Operations will be informed and decide the necessary action to take.

12 Emails

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

12.2 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.

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

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

12.5 Any email that contains sensitive or personal information is only sent using secure and encrypted email or via a secure portal for example, Sofie or Egress.

12.6 Staff members and pupils are required to block any spam and junk mail which they receive (ie. that has not been automatically blocked).

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

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

13 Social Networking

13.1 Personal use

13.1.1 Access to social networking sites is filtered as appropriate.

13.1.2 Staff and pupils are not permitted to use social media for personal use at any time whilst in school.

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

13.1.4 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.

13.1.5 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 close family friends with a parent at the school, they will disclose this to the DSL and Headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

13.1.5 Staff receive induction information on how to use social media safely and sign a code of conduct every year.

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

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

13.2 Use on Behalf of the School

13.2.1 The school or trust’s official social media channels are only used for official educational or engagement purposes.

13.2.2 Staff members must be authorised by the Headteacher to access to the school’s social media accounts or the CEO in respect of trust social media channels.

13.2.3 All communication on official social media channels by staff on behalf of the school or trust must be clear, transparent, and open to scrutiny. Care must be taken with regards to the wording and content of posts.

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

14 School and Trust Websites

15.1 The Director of Finance & Operations (DFO) and Headteachers have responsibility for the overall content of the trust and school websites, ensuring the content is appropriate, accurate, up-to-date and meets government requirements. They must ensure:

- The websites 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 the necessary permissions have previously been granted and provisions in the Photography Policy are met.

15 Use of School-Owned Devices

15.1 Pupils

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

15.1.2 School-owned devices must be used in accordance with the Acceptable Use of Technology Pupil Agreement.

15.2 Staff

15.2.1 Members of staff members may be issued with a laptop or Ipad to assist with their work.

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

15.2.3 All school/trust-owned devices are password protected.

15.2.4 All school/trust-owned devices are fitted with software to ensure they can be remotely accessed in case data on the device needs to be protected, retrieved, or erased.

15.2.5 Devices must be locked if the user leaves their desk of if left inactive for a period of time.

15.2.6 Devices must not be shared with family or friends

15.2.7 Work devices must be solely used for work activities

15.2.8 The IT Support provider reviews all school/trust-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

15.2.9 No software, apps or other programmes can be downloaded onto a device without authorisation from the IT Support Provider.

15.2.10 Staff members found to be misusing school-owned devices will be managed in line with the Trust's Disciplinary Policy and Procedure.

16 Use of Personal Devices

16.1 Pupils

16.1.1 Pupils are not permitted to use their personal devices in school-during lesson time or when moving between lessons.

16.1.2 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.

16.1.3 The Headteacher and the DSL may authorise the use of mobile devices by a pupil for safety or precautionary use.

16.1.4 Pupils' devices can only be searched by the DSL/DDSL's, in accordance with the DfE's guidance on searching, screening and confiscation. Phones may be confiscated by school staff and locked securely away if the AUP has been breached.

16.1.5 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 DSL/DDSL's to be handed to the police.

16.2 Staff

16.2.1 Staff members are not permitted to use their **personal devices in view of the pupils and/or** during lesson time, other than in an emergency or **for medical purposes e.g. blood sugar level monitoring.**

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

- Toilets
- Changing rooms

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

16.2.4 Staff members report should report any concerns about their colleagues' use of personal devices on the school premises in line with the Whistleblowing Policy.

16.2.5 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 DSL/Headteacher will inform the police and action will be taken in line with the Trust's Disciplinary Policy and Procedures.

16.2.6 Appropriate signage and a visitors agreement leaflet is displayed/available to inform visitors to the school of the expected use of personal devices.

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

17 Remote Learning

17.1. All remote learning is delivered in line with the individual schools' Supported Home Learning Guidance

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.
- Not record, store, or distribute video material without permission.
- 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.
- Ensure all Teams calls are recorded and make all participants aware of this.

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 Headteacher/Deputy Head. 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. appropriately will be sanctioned and dealt with according to the Acceptable Use 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 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.

17.8. 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.

17.9. 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.
- Advise parents to monitor their child’s online use and be aware of the content of their online activities.

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

18 Managing reports of online safety incidents

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

- Emails to all staff
- Staff meetings
- Staff training
- The ICT curriculum (online safety two terms per year)
- Assemblies

18.2 Concerns regarding a staff member's online behaviour should be reported to the DSL/Headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Professional Code of Conduct & Disciplinary Policy and Procedures.

18.3 Concerns regarding a pupil's online behaviour are reported to the DSL**/**DDSL's who investigates concerns with the IT Support Provider.

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

18.5 Where there is a concern that illegal activity has taken place, the DSL/Headteacher contacts the police.

18.6 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. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

18.7 All online safety incidents and the school's response are recorded on CPOMS and monitored by the DSL and Online Safety lead.

18.8 **Appendix A** of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and child-on-child abuse.

19 Policy monitoring and review

19.1 Enable Trust recognises that the online world is constantly changing; therefore, the school's DSLs, Online Safety Leads and the Headteacher, in conjunction with the IT Support Provider will conduct annual reviews of this policy to evaluate its effectiveness. This will be supported by an annual risk assessment that considers and reflects the risks faced by our schools' communities.

19.2 The governing board, Headteacher, DSL, Online Safety Lead and DFO review this policy in full on an annual basis and following any online safety incidents. The updated policy will be recommendations to the Board of Trustees for approval.

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

Appendix 1 - Responding to Specific Online Safety Concerns

1. Cyberbullying

- Cyberbullying, against both pupils and staff, is not tolerated.
- Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.
- Information about the trust's full response to incidents of cyberbullying can be found in the Anti-Bullying Policy.

2. Online sexual violence and sexual harassment between children (child-on-child abuse)

- The trust recognises that child-on-child 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

- Our schools will respond to any concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school-owned equipment.
- Concerns regarding online child-on-child abuse must be reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.
- Information about the full response to incidents of online child-on-child abuse can be found in the Child Protection and Safeguarding Policy.

3. Upskirting

- 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.
- 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.

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

- Upskirting is not tolerated by the trust. Any incidents of upskirting will be 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.

4. Sexting and the sharing of indecent imagery of pupils

Please also refer to section 7.9 of the Trust’s Safeguarding and Child Protection Policy.

- Sharing indecent 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.

- Any concerns regarding sexting will be reported to the DSL.

- The DSL will use their professional judgement, in line with the Child Protection and Safeguarding Policy, to determine whether the incident is experimental, i.e. expected for the developmental stage of the pupils involved, or aggravated, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the pupil depicted.

- Where the incident is categorised as ‘experimental’, the pupils involved will be supported in the understanding to prevent future incidents.

- Where there is reason to believe the incident will cause harm to the pupil depicted, or where the incident is classified as ‘aggravated’, the following process is followed:

- The DSL or Online Safety lead holds an initial review meeting with appropriate school staff

- Subsequent interviews will be held with the pupils involved, if appropriate

- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm

- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children’s social care services and/or the police immediately

- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

- When investigating a report, staff members will not view nude and semi-nude images and will report immediately to the DSL/DDSL’s.

- If a decision is made to view the imagery, the DSL will be satisfied that viewing:
  - Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any pupil involved.
  - Is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the pupil in taking down the image or in making a report.
  - Is unavoidable because a pupil has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.
  - Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the DSL's professional judgement.
  - Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.
  - Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

5. Online abuse and exploitation

- Through the online safety and PSHE curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- Schools will respond to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, must be reported to the DSL, and dealt with in line with the Child Protection and Safeguarding Policy.

6. Online hate

- The trust and its schools will not tolerate online hate content directed towards or posted by members of the school community.
- Incidents of online hate will be 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.

7. Online radicalisation and extremism

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

- 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.

8. Artificial Intelligence (AI)

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- Enable Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- The Trust and its schools will treat any use of AI to bully pupils in line with our Anti-bullying/behaviour policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.