1. Legal framework

1.1. This policy has due regard to all relevant legislation and guidance including, but

Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with Special Educational Needs or Disabilities (SEND) face online.

Liaising with relevant members of staff on online safety matters, e.g. the SENCo and Central IT Team.

Ensuring online safety is recognised as part of the schoolôs safeguarding responsibilities and that a coordinated approach is implemented.

Ensuring safeguarding is considered in the schoolôs approach to remote learning.

Staying up-to-date with current research, legislation and online trends.

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 schoolôs provision, and using this data to update theschoolôs procedures.

Reporting to the Principal about online safety on a regularly basis.

2.4. ICT School Leads (or designated Senior Leader)

Taking the lead responsibility for online safety in the school.

Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

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.

Coordinating the schoolôs participation in local and national online safety events, e.g. Safer Internet Day.

Taking responsibility for the security of ICT systems and electronic data they use or have access to.
Modelling good online behaviours.
Maintaining a professional level of conduct in their personal use of technology.
Having an awareness of online safety issues.
Reporting concerns in line with the schoolôs reporting procedure.
Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.7. Pupils are responsible for:

Adhering to this policy, the Acceptable Use Agreement and other

3.6. The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.
3.7. The ICT Lead is involved with the development of the schoolôs online

4.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners[1].
4.3. In addition to this training, staff also receive regular online safetyupdates as required and at least annually.
4.4. The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

Tablets/iPads/iPods
Google Classroom
Email
Cameras

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.
6.3. Class teachers ensure that any internet-derived materials are used in line with copyright law.
6.4. Pupils are supervised when using online materials during lesson time, suitable to their age and ability.

7. Internet access

7.1. Pupils, staff and other members of the school community are only granted access to the schoolôs internet network once they have read and signed the Acceptable Use Agreement.
7.2. A record is kept of users who have been granted internet access.
7.3. All members of the school community are encouraged to use the schoolôs WIFI network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

8.1. The Central IT Team ensures the schoolôs ICT network has appropriate filters and monitoring systems in place.
8.2. The Central IT Team undertake a risk assessment to determine what filtering and monitoring systems are required.
8.3. The filtering and monitoring systems the school implements are appropriate to pupilsôages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
8.4. The Central IT Team ensures ôover blockingô does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
8.5. Central IT Team undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.
8.6. Requests regarding making changes

10.1. Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement.
10.2. Staff and pupils are given approved school email accounts and are only able to use these accounts when doing school-related work.
10.3. Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant ICT Acceptable Use Agreement.
10.4. Personal email accounts are not permitted to be used on school devices nor in lessons/the company of pupils/parents.
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 as appropriate.
10.7. The schoolôs monitoring system can detect inappropriate links, malware and profanity within emails ï staff and pupils are made aware of this.
10.8. Chain letters, spam and all other emails from unknown sources are deleted without being opened.
10.9. The ICT Lead organises annual workshops where they explain what a phishing email and other malicious emails might look like ï this may include links with local partners such as Warning Zone.
10.10. Any cyberattacks initiated through emails are managed by Central IT Team.

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 members are advised that their conduct on social media can have an impact on their role and reputation within the school.
11.4. Staff receive annual training on how to use social media safely and responsibly.
11.5. Staff are not permitted to communicate on business matters with pupils or parents over social networking sites and are advised 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 responsiblythrough 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 Principal and managed in accordance with the relevant policy - Anti-Bullying and Cyberbullying Policy, Code of Conduct and School Behaviour policies.

Use on behalf of the school

11.8. The use of social media on behalf of the school is conducted in line with the Acceptable Use Agreement.
11.9. The schoolôs official social media channels are only used for official educational or engagement purposes.
11.10. Staff members must be authorised by the Principal to access to the schoolôs 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

14.4. Staff members report concerns about their colleaguesô use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy.
14.5. 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 will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.
14.6. The Principal may authorise the use of mobile devices by a pupil for safety or precautionary use.
14.7. Pupilsô devices can be searched, screened and confiscated in accordance with the Acceptable Use Agreement.
14.8. If a staff member reasonably believes a pupilôs 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.
14.9. Any concerns about visitorsô use of personal devices on the school premises are reported immediately to the Principal and/or 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
- Workshops for Parents
- Class visits and visitors such as Warning Zone

15.2. Concerns regarding a staff memberôs online behaviour are reported to the Principal who decides on the best course of action in line with the relevant policies.
15.3. Concerns regarding a pupilôs online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the Principal and Central IT Team.
15.4. Where there is a concern that illegal activity has taken place, the Principal or DSL contacts the police.
15.5. All online safety incidents and the schoolôs response are recorded using CPOMS/MyConcern.

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

0 g0 G[(sta)-5(ff)] TJETQ0.000008875 0 595.56 842.04 re54 nBW*T/F6 12 Tf1 [(b.35 Tm0(o)6(f)-2-3(ff)-3

16.4. Concerns regarding Peer-on-peer abuse, upskirting, sexting are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Online abuse and exploitation

16.5. 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.

16.6. 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.

16.7. 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

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

16.9. 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

16.10. The schoolôs filtering system aims to protect pupils and staff from viewing extremist content.

16.11. 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.

17. Remote learning policy

17.1. Guidance for all staff and pupils using video/audio communication:

- Communicate in groups ï one-to-one sessions are only carried out where necessary.
- Wear suitable clothing ï this includes others in the household.
- Be situated in a suitable ópublicôliving area within the home with an appropriate background during video communication.
- Use appropriate language ï this includes others in the household.
- Maintain the standard of behaviour expected.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video/audio material without permission.
- Report any issues/concerns with internet connections to avoid disruption to lessons.
- Always remain aware that they are visible.

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.

17.5. Pupils not using devices or software as intended will

Appendix 1: Online harms and risks curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in

Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain.

Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why That it is okay to say no and to not take part in a challenge How and where to go for help The importance of telling an adult about challenges which include threats or secrecy ï œchain letterôstyle challenges	This risk or harm is covered in the following curriculum area(s): Å Relationships education Å Health education
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: That online content (sometimes gang related) can glamorise the possession of weapons and drugs That to intentionally encourage or assist in an offence is also a criminal offence How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): Å Relationships education Å **[Secondary schools]** RSE
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: That, in some cases, profiles may be people posing as someone they are not	

Appendix 2: Policies associated with online safety and remote learning

Acceptable Use Agreement
Anti-bullying and Cyberbullying Policy
Behaviour Policy
Behaviour principles written statement
Child Protection and Safeguarding Policy
Code of Conduct
Data Breach Procedure
Data Protection Policy
Disciplinary Policy and Procedures
PSHE Policy
RSE and Health Education Policy