2.1. The Avanti Schools Trust (AST) is responsible for:

- Ensuring that this policy is effective

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 12 Tf1 0 0 1 427.18 692.14 Tm0 g0 G[( )]

2.8. Parents are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Discussing the safe use of the computer, network, mobile phones, Internet access and other new technologies with their children.
- Reporting any concerns to the Principal.

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

- RSE
- Health education
- PSHE and Citizenship
- Computing

3.2. The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

3.3. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

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

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

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

3.6. The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

3.7. The ICT Lead 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 Looked After Children (LAC). Relevant membersof staff, e.g. the SENCo and designated teacher for LAC, work togetherto 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 Principal and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

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

3.12. Lessons [redacted]~~es are planned carefully so~~ [redacted]

4.2. Online safety training for staff is ensure their child understands the document and the implications of not following it.

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

- Computers
- Laptops
- 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.

7.1. Pupils, staff, and other members of the school community are only granted access to the school’s internet network once they have readluding

9.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by the Central IT Team.

9.2. Firewalls are switched on at all times.

9.3. The Central IT Team review the firewalls on a regular basis

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

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

10.9. The ICT Lead organises annual workshops where they explain what a phishing email and other malicious emails might look like – this may include links with local partners such as Warning Zone.

10.10. Any cyberattacks initiated through emails are managed by Central IT Team.

11.1. 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 ov -5(afpan /<MCID 39/Lang du)-7(BT/F3 12 Tf1 0 0 1 176.81 495.31 Tm0 g0 G[( )] TJE

settings to ensure p re not able to contact them on social media.

11.6. Pupils are taught how to us online safety curriculum.

11.7. Concerns regarding the /F3 12 b g0 G[(c)3(u) 00008875 0 595

13.1.

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. Pupils' devices can be searched, screened, and confiscated in accordance with the Acceptable Use Agreement.

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

14.9. Any concerns about visitors' use of personal devices on the school premises are reported immediately to the Principal and/or DSL.

15.1. Staff members and pupils are informed abou4 reW* nBT/F6 12 Tf1 0 0 1 147.02 575.47 Tr

16.3. Information about the school's full response to incidents of cyberbullying can be found in the School Behaviour Policy, Anti-bullying and Cyberbullying Policy.

- Use appropriate language – 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 be disciplined in line with the Acceptable Use Agreement.

17.6. The school will risk assess the technology used for remote learning prior to use to minimise privacy issues or scope for inappropriate use.

17.7. The school will communicate with parents about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

17.8. 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 school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

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

Disinformation, misinformati on and hoaxes	• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleadinginformation can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons

Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images, and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed/targeted/groomed as aresult of interacting with a fake website or scam email • Who pupils should go to for support	This risk or harm is covered in the following curriculum area(s): Relationships education RSE Health education Computing curriculum
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum area(s): Relationships education Computing curriculum
Password phishing	Password phishing is the process by which people try to find out individuals'passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum area(s): Relationships education Computing curriculum
	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s):

Personal data	- How cookies work - How data is farmed from sources which look neutral - How and why personal data is shared by online companies - How pupils can protect themselves and that acting quickly is essential when something happens - The rights children have with regards to their data - How to limit the data companies can gather	Relationships education RSE Computing curriculum

Some online behaviours are abusive. They are negative in nature,potentially harmful and, in some cases, can be illegal.

Teaching includes the follow08.23 279q115.34 488.59F:88BDC q115.

Online abuse

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 – 'chain letter' style challenges	This risk or harm is covered in the following curriculum area(s): Relationships education 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 inviolence	This risk or harm is covered in the following curriculum area(s): Relationships education 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 or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): Relationshipseducation Computing curriculum

Grooming	Knowing about the different types of grooming and motivations for it, e.g.radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines). Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum area(s): Relationshipseducation RSE

	or arranging to meet someone they have not met before - What online consent is and how to develop strategies to confidently say no to both friends and strangers online	Computing curriculum

Impact on confidence (including body confidence)	Knowing about the impact of comparisons to ‘unrealistic’ online images.Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers •

Reputational damage	What users post can affect future career opportunities and relationships –both positively and negatively. Teaching includes the following: • Strategies for positive