AVANTI SCHOOLS TRUST

This is a Category 1 Trust Level 1 Policy:

(Operationally delegated and applied Trust-wide)

This policy is in force until further notice from:	1st Feb 2023
This policy must be reviewed by:	Spring 2024
Policy Author(s):	Mike Ion
Date	

All schools within the Trust understand 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:

- : Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- : Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- : 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. This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

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 aConnected 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 all school policies (see Appendix 2)

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

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the school Designated Safeguarding Lead's (DSL) 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 there are appropriate filtering and monitoring systems in place in its schools.

cont2 is7(e5(ls.)] TJETQ0.000008375 0 5[illegible]

D nd conc - -

- fEny.

AfH@ D@

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 school's participation in local and national online safety events, e.g. Safer Internet Day.
- Raise technical issues with the Central IT Team and collaborate with them to achieve a solution.

2.5. Central IT Team are responsible for:

- Ensuring online safety configurations are audited and evaluated.
- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Working with the DSL and Principal to conduct half-termly light-touch reviews of this policy.

2.6. All staff are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- 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.

2.7. Pupils are responsible

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

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 o

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 safety updates 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.

4.5. 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.

4.6. All staff to confirm they have read and understand this policy upon their induction and are informed of any changes.

4.7. Staff are required to adhere to the Code of Conduct policy at all times.

4.8. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

4.9. The DSL and/or the ICT Lead acts as the first point of contact for staff requiring advice about online safety.

5.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.

5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' Workshops (school staff and NSPCC)
- Coffee Mornings
- Email communications (newsletters, letters etc…)
- Website
- Twitter

5.3. Parents are directed to the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to

ensure their child understands the document and the implications of not following it.

6.1. 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,

8.3. The filtering and monitoring systems the school implements 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.

8.4. The Central IT Team ensures 'over blocking' 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 to the filtering system are directed to the Principal.

8.7. Prior to making any changes to the filtering system, Central IT Team conduct

9.1.

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

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 Principal and managed in accordance with the relevant policy - Anti-Bullying and Cyberbullying Policy, Code of Conduct and School Behaviour policies.

11.8. The use of social media on behalf of the school is conducted in line with the Acceptable Use Agreement.

11.9. The school's official social media channels are

13.1. Staff members have access to and may be issued with various devices to assist with their work.

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

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

16.3. Information about the school's full response to

- 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.

0078} TETQ0.000008875 0 595.56 842.04 reW* nBT/F6 175 0 595.56 842.04 reW122.14T/F3 12 Tf

17.7. The school will communicate with parents about what methods of deliveringq0.000008875 0

Some online activities have age

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 • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	Relationships education Health education RSE Computing curriculum Citizenship

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

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

Teaching includes the following:

Online abuse

- The types of online abuse, including sexual harassment, bullying,trolling and intimidation
- When online abuse can become illegal
- How to respond to online abuse and how to access support
- How to respond when the abuse is anonymous
- The potential implications of online abuse

Knowing about the different types of grooming and motivations for it, e.g.

Grooming

or arranging to meet someone they have not met

Impact on confidence (including body confidence)

Reputational damage	What users post can affect future career opportunities and relationships –both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): RSE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	