# AVANTI SCHOOLS TRUST

## Online Safety & Remote Learning Policy

• • • • • • • • •

### Spring 2023

*Review date: Autumn 2025*

# ONLINE SAFETY AND REMOTE LEARNING POLICY

This Policy is a Category 1 Policy (Full Delegation)

| | |
|---|---|
| This policy is in force until further notice from: | Spring 2023 |
| This policy must be reviewed by no later than*: <br><br> *this refers to the term in which the Policy must be reviewed by the appropriate Committee for recommendation to the Board. | Autumn 2025 |
| Policy Author(s): | CEO |
| Date policy reviewed by Committee and Minute reference | Learning, Teaching & Standards Committee: <br> 14.10.24 <br> (Minute reference 16) |
| Date Policy approved by the Trust Board and Minute reference | 01.02.23 <br> (Minute reference 61) |
| Location of publication of policy: | Governor Hub/ <br> AST Website/ <br> Internal Records and Intranet |

**Statement of Intent**

All schools within the Trust understand that using online services is an important aspect of raising educational standards, promoting 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 children and young people 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 or radical or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users. E.g. commercial advertisings 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 children and young people, and staff resolve 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 children and young people 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) "Keeping 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 all school policies (see Appendix 2)

## 2. Roles and Responsibilities

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.

2.2. The Principal is responsible for:

- Supporting the DSL and any deputies, ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Working with the DSL and Central IT Team to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and AST to update this policy on an annual basis.

2.3. The DSL is responsible for:

- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they can understand the risks associated with online safety and can recognise additional risks that children and young people 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 school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's 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 school's provision and using this data to update the school's procedures.
- Reporting to the Principal about online safety on a regular 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 children and young people 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 children and young people 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 children and young people 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.   Children and young people 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 has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

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.   The curriculum

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.   Children and young people 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 children and young people' ages and developmental stages.

3.5.   The underpinning knowledge and behaviours children and young people 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 children and young people may face online are always considered when developing the curriculum. The risks that are considered and how they are covered 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 children and young people who may be more susceptible to online harm or have less support from family and friends in staying safe online. E.g. children and young people with SEND and Looked After Children (LAC). Relevant members of staff, e.g. the SENCo and designated teacher for LAC, work together to ensure the curriculum is tailored so these children and young people 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 children and young people. 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 children and young people?
- Are they appropriate for children and young people' 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 should consider the topic that is being covered and the potential that children and young people in the class have suffered or may be suffering from online abuse or harm in this way. The DSL should advise 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 children and young people 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 children and young people raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

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

4.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners (local authorities, chief officers of police, and clinical commissioning groups).

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 children and young people safe while they are online at school.
- Recognise the additional risks that children and young people with SEND face online and offer them support to stay safe online.

4.6. All staff are to confirm they have read and understood this policy upon their induction and are informed on 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.    Educating parents

5.1.    The school works in partnership with parents to ensure children and young people 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.    Classroom use

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 children and young people 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. Children and young people are supervised when using online materials during lesson time, suitable to their age and ability.

## 7. Internet access

7.1. Children and young people, staff, and other members of the school community are only granted access to the school's 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 school's 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 school's 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 children and young people's ages, the number of children and young people using the network, how often children and young people 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 children and young people can be taught with regards to online teaching and safeguarding.

8.5. The Central IT team undertakes 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, the Central IT Team conduct a risk assessment, in collaboration with the Principal, DSL and/or ICT Lead.

8.8. Any changes made to the system are recorded by the Central IT Team.

8.9. Reports of inappropriate websites or materials are made to the DSL and Central IT Team immediately, who investigates the matter and makes any necessary changes.

8.10. Deliberate breaches of the filtering system are reported to the DSL and Central IT Team, who will escalate the matter appropriately.

8.11. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Acceptable Use Agreement.

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

8.13. 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.

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

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

8.16. Concerns identified through monitoring are reported to the Central IT Team that 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 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 to ensure they are running correctly, and to carry out any required updates.

9.4. Staff and children and young people are advised not to download unapproved software or open unfamiliar email attachments.

9.5. Staff members and children and young people report all malware and virus attacks to the ICT Lead and if appropriate, the Principal.

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

9.7.    All children and young people are provided with their own unique username and private passwords for the organisation's Google Suite (Classroom).

9.8.    Staff members and children and young people are responsible for keeping their passwords private.

9.9.    Passwords have a minimum and maximum length and require a mixture of characters to ensure they are as secure as possible.

9.10.   Password resets will be encouraged at least termly.

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 log out of devices when they are not in use.

9.13.   Users inform the appropriate staff 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 procedures in the ICT Acceptable Use Agreement will be followed.

9.15.   Full details of the school's network security measures can be requested from the Central IT Team.

## 10.    Emails

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 children and young people 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 children and young people 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 children and young people/parents.

10.5.   Any email that contains sensitive or personal information is only sent using secure and encrypted email.

10.6. Staff members and children and young people 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 children and young people 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 cyber-attacks initiated through emails are managed by the Central IT Team.

## 11. Social networking

Personal Use

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

11.2. Staff and children and young people 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 children and young people or parents over social networking sites and are advised to alter their privacy settings to ensure children and young people and parents are not able to contact them on social media.

11.6. Children and young people 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 only used for official educational or engagement purposes.

11.10.   Staff members must be authorised by the Principal to have 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 policy 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.    Staff are clear on the procedure to escalate any concerns relating to information on the school website.

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 children and young people is not published on the website.

12.4.    Images and videos are only posted on the website if the provisions in the Acceptable Use Agreement are met.

## 13.    Use of school-owned devices

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

13.2.    Children and young people 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 Learning.

13.3.    School-owned devices are used in accordance with the Acceptable Use Agreement.

13.4.    All school-owned devices are password protected.

13.5.    All school-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.

13.6.    The Central IT Team review all school-owned devices on a regular basis to carry out software updates and maintenance.

13.7.    No software, apps or other programmes can be downloaded onto a device without the Central IT Team.

13.8.    Staff members or children and young people found to be misusing school-owned devices are disciplined in line with the staff Code of Conduct, Acceptable Use Agreement and Behaviour Policy.

## 14.    Use of personal devices

14.1.    Personal staff devices are used in accordance with the Acceptable Use Agreement. Any personal electronic device that is brought into school by a staff member is the responsibility of the user.

14.2.    Devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

14.3.    Staff members are not permitted to use their personal devices or take photos or videos of children and young people.

14.4.    Staff members report concerns about their colleagues' 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.    Children and young peoples' 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. Managing reports of online safety incidents

15.1. Staff members and children and young people 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 member's 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 pupil's 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 school's response are recorded using CPOMS/MyConcern.

## 16. Responding to specific online safety concerns

Cyberbullying

16.1. Cyberbullying, against both children and young people and staff, is not tolerated.

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

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.

Peer-on-peer abuse, Upskirting and Youth produced sexual imagery (sexting)

Online Abuse and exploitation

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

16.5. 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.

16.6. 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

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

16.8. 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

16.9. The school's filtering system aims to protect children and young people and staff from viewing extremist content.

16.10. 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.

16.11. 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.

## 17. Remote learning policy

17.1. Guidance for all staff and children and young people using video/audio communication:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in the household.

- Be situated in a suitable "public" living area within the home with an appropriate background during video communication.
- 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 children and young people with SEND. This will be decided and approved by the SLT.

17.5. Children and young people 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. Alternative 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.

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


## 18. Monitoring and review

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

## Appendix 1: Online harms and risks – curriculum coverage

| Subject area | Description and teaching content | Curriculum area the harm or risk is covered in |
|---|---|---|
| **How to navigate the internet and manage information** | | |
| Age restrictions | Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.<br><br>Teaching includes the following:<br><br>• That age verification exists and why some online platforms ask users to verify their age.<br>• Why age restrictions exist.<br>• That content that requires age verification can be damaging to under-age consumers.<br>• What the age of digital consent is (13 for most platforms) and why it is important. | This risk or harm is covered in the following curriculum area(s):<br><br>• Health education<br>• Computing curriculum |
| How content can be used or shared | Knowing what happens to information, comments or images that are put online.<br><br>Teaching includes the following:<br><br>• What a digital footprint is, how it develops and how it can affect children and young people's futures.<br>• How cookies work.<br>• How content can be shared, tagged and traced.<br>• How difficult it is to remove something once it has been shared online.<br>• What is illegal online. E.g. youth-produced sexual imagery (sexting). | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• Health education<br>• (Secondary schools) RSE<br>• Computing curriculum |
| Disinformation, misinformation and hoaxes | Some information shared online is accidently or intentionally wrong, misleading or exaggerated. | This risk or harm is covered in the following curriculum area(s): |

| | Teaching includes the following: | |
|---|---|---|
| | • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive.<br>• Misinformation and being aware that false and misleading information can be shared inadvertently.<br>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons.<br>• 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.<br>• How to measure and check authenticity online.<br>• The potential consequences of sharing information that may not be true. | • Relationships education<br>• Health education<br>• (Secondary schools) RSA<br>• Computing curriculum<br>• (KS3 and KS4) 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.<br><br>Teaching includes the following:<br><br>• How to recognise fake URLs and websites.<br>• What secure markings on websites are and how to assess the sources of emails.<br>• The risks of entering information to a website, which is not secure.<br>• What children and young people should do if they are harmed/targeted/groomed as a | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• (Secondary schools) RSE<br>• Health education<br>• Computing curriculum |

| | | |
|---|---|---|
| | result of interacting with a fake website or scam email.<br>• Who children and young people should go to for support. | |
| Online Fraud | Fraud can take place online and can have serious consequences for individuals and organisations.<br><br>Teaching includes the following:<br><br>• What identity fraud, scams and phishing are.<br>• That children are sometimes targeted to access adults' data.<br>• 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):<br><br>• Relationships education<br>• Computing curriculum |
| Password phishing | Password phishing is the process by which people try to find out individual's passwords so they can access protected content.<br><br>Teaching includes the following:<br><br>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them.<br>• How to recognise phishing scams.<br>• The importance of online security to protect against viruses that are designed to gain access to password information.<br>• 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):<br><br>• Relationships education<br>• Computing curriculum |
| Personal Data | Online platforms and search engines gather personal data – this is often referred to as "harvesting" or "farming."<br><br>Teaching includes the following: | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education |

| | | |
|---|---|---|
| | • How cookies work<br>• How data is farmed from sources which look neutral.<br>• How and why personal data is shared by online companies.<br>• How children and young people can protect themselves and that acting quickly is essential when something happens.<br>• The rights children have with regards to their data.<br>• How to limit the data companies can gather. | • (Secondary schools) RSE<br>• Computing curriculum |
| Persuasive design | Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.<br><br>Teaching includes the following:<br><br>• That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online as long as possible.<br>• How notifications are used to pull users back online. | This risk or harm is covered in the following curriculum area(s):<br><br>• Health education<br>• Computing curriculum |
| Privacy settings | Almost all devices, websites, apps, and other online services come with privacy settings that can be used to control what is shared.<br><br>Teaching includes the following:<br><br>• How to find information about privacy settings on various devices and platforms.<br>• That privacy settings have limitations. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• Computing curriculum |

| Targeting of online content | Much of the information seen online is a result of some form of targeting. Teaching includes the following:<br><br>• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts.<br>• How the targeting is done.<br>• The concept of clickbait and how companies can use it to draw people to their sites and services. | This risk or harm is covered in the following curriculum area(s):<br><br>• Health education<br>• Computing curriculum |
|---|---|---|
| **How to stay safe online** | | |
| Online abuse | Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal.<br><br>Teaching includes the following:<br><br>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation.<br>• When online abuse can become illegal.<br>• How to respond to online abuse and how to access support.<br>• How to respond when the abuse is anonymous.<br>• The potential implications of online abuse.<br>• What acceptable and unacceptable online behaviours look like. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• (Secondary schools) RSE<br>• Health education<br>• Computing curriculum<br>• (KS4) citizenship |
| Challenges | Online challenges acquire mass followings and encourage others to take part in what they suggest.<br><br>Teaching includes the following:<br><br>• What an online challenge is and that, while some will be fun and harmless, | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• Health education |

| | | |
|---|---|---|
| | others may be dangerous and even illegal.<br>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why.<br>• That it is okay to say no and to not take part in a challenge.<br>• How and where to go for help.<br>• The importance of telling an adult about challenges which include threats or secrecy – "chain letter" style challenges. | |
| Content which incites | Knowing that violence can be incited online and escalate very quickly into offline violence.<br><br>Teaching includes the following:<br><br>• The online content (sometimes gang related) can glamorise the possession of weapons and drugs.<br>• That to intentionally encourage or assist in an offence is also a criminal offence.<br>• 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):<br><br>• Relationships education<br>• (Secondary schools) RSE |
| Fake profiles | Not everyone online is who they say they are.<br><br>Teaching includes the following:<br><br>• That, in some cases, profiles may be people posing as someone they are not or may be "bots."<br>• How to look out for fake profiles. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• Computing curriculum |
| Grooming | Knowing about the different types of grooming and motivations for it. E.g. | This risk or harm covered in the following curriculum area(s): |

| | | |
|---|---|---|
| | radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines).<br><br>Teaching includes the following:<br><br>• Boundaries in friendships with peers, in families, and with others.<br>• Key indicators of grooming behaviour.<br>• The importance of disengaging from contact with suspected grooming and telling a trusted adult.<br>• How and where to report grooming both in school and to the police.<br><br>At all stages, it is important to balance teaching children and young people 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. | • Relationship education<br>• (Secondary schools) RSE |
| Live streaming | Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it.<br><br>Teaching includes the following:<br><br>• What risks of carrying out live streaming are. E.g. the potential for people to record livestreams and share the content.<br>• The importance of thinking carefully about who the audience might be and if children and young people would be comfortable with whatever they are streaming being shared widely.<br>• That online behaviours should mirror offline behaviours and that this | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• (Secondary schools) Health Education |

| | | |
|---|---|---|
| | should be considered when making a livestream.<br>• That children and young people should not feel pressured to do something online that they would not do offline.<br>• Why people sometimes do and say things online that they would never consider appropriate offline.<br>• The risk of watching videos that are being livestreamed. E.g. there is no way of knowing what will be shown next.<br>• The risks of grooming. | |
| Pornography | Knowing that sexually explicit materials present a distorted picture of sexual behaviours.<br><br>Teaching includes the following:<br><br>• That pornography is not an accurate portrayal of adult sexual relationships.<br>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour.<br>• That not all people featured in pornographic material are doing so willingly. I.e. revenge porn or people trafficked into sex work. | This risk or harm is covered in the following curriculum area(s):<br><br>• (Secondary schools) RSE |
| Unsafe communication | Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met.<br><br>Teaching includes the following:<br><br>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education<br>• (Secondary schools) RSE<br>• Computing curriculum |

| | • How to identify indicators of risk and unsafe communications.<br>• The risks associated with giving out addresses, phone numbers or email addresses to people children and young people do not know or arranging to meet someone they have not met before.<br>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online. | |
|---|---|---|
| **Wellbeing** | | |
| Impact on confidence (including body confidence) | Knowing about the impact of comparisons to "unrealistic" online images.<br><br>Teaching includes the following:<br><br>• The issue of using image filters and digital enhancement.<br>• The role of social media influencers, including that they are paid to influence the behaviour of their followers.<br>• The issue of photo manipulation, including why people do it and how to look out for it. | The risk or harm is covered in the following curriculum area(s):<br><br>• (Secondary schools) Health education |
| Impact on the quality of life, physical and mental health and relationships | Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline.<br><br>Teaching includes the following:<br><br>• How to evaluate critically what children and young people are doing online, why they are doing it and for how long (screen time).<br>• How to consider quality v. quantity of online activity. | This risk or harm is covered in the following curriculum area(s):<br><br>• Health education |

| | | |
|---|---|---|
| | • The need for children and young people to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear of missing out.<br>• That time spent online gives users less time to do other activities, which can lead to some users to become physically inactive.<br>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues.<br>• That isolation and loneliness can affect children and young people and that it is very important for them to discuss their feelings with an adult and seek support.<br>• Where to get help. | |
| Online vs. offline behaviours | People can often behave differently online to how they would act face to face.<br><br>Teaching includes the following:<br><br>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives.<br>• How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face. | This risk or harm is covered in the following curriculum area(s):<br><br>• Relationships education |
| Reputational damage | What users post can affect future career opportunities and relationships – both positively and negatively.<br><br>Teaching includes the following:<br><br>• Strategies for positive use. | This risk or harm is covered in the following curriculum area(s):<br><br>• Secondary schools (RSE) |

| | | |
|---|---|---|
| | • How to build a professional online profile. | |
| Suicide, self-harm and eating disorders | Children and young people 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 children and young people and should take care to avoid giving instructions or methods and avoid using language, videos and images. | |

**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
- PHSE Policy
- RSE and Health Education Policy