



## The Societas Trust:

## Primary Academy

# Online Safety Policy

Date of Policy	2023
Reviewed and Agreed by	The Directors' Board
Review Date	12 July 2023
Next Review Date	Summer 2024

## Contents:

### Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Generative artificial intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

### **Appendix**

[Appendix 1: Online Safety Rules and Consent](#)

[Appendix 2: Online Safety Posters – Key Stages One and Two](#)

[Appendix 3: Staff Acceptable Use Agreement / Code of conduct](#)

[Appendix 4: Online harms and risks – curriculum coverage](#)

## Statement of intent

**Name of school** understands 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 four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

## 1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy
- Teaching and Learning

## 2. Roles and responsibilities

The Directors' board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Supporting the DSL (if not the head teacher) and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the DSL and Directors' board to update this policy on an **annual** basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a **termly** basis.
- Working with the headteacher and ICT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the headteacher and Directors' board to update this policy on an **annual** basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct **half-termly** light-touch reviews of this policy.

All staff members will be 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- 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.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

### **3. Managing online safety**

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- The online safety curriculum
- Assemblies

### **Handling online safety concerns**

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies e.g. Code of Conduct for Adults, Confidential Reporting Policy, Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and

manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

## **4. Cyberbullying**

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

## **5. Child-on-child sexual abuse and harassment**

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence



- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

## **Upskirting**

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

## **Youth produced sexual imagery (sexting)**

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the DSL.

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

- The DSL holds an initial review meeting with appropriate school staff;
- Subsequent interviews are held with the pupils involved, if appropriate;
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm;

- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately;
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented.

Investigating a report, staff members will not view nude and semi-nude images unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view nude or semi-nude imagery as part of an investigation, they discuss this with the DSL and headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

If a decision is made to view the imagery, the DSL will be satisfied that viewing:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any pupil involved.
- Is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the pupil in taking down the image or in making a report.
- Is unavoidable because a pupil has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.

Where it is necessary to view the imagery the DSL will:

- Never copy, print, share, store or save images; this is illegal.
- Discuss the decision with the headteacher.
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team with delegated authority from the headteacher.
- Make sure viewing takes place with the headteacher or another member of the SLT in the room; additional people in the room will not view the imagery.
- Only view the imagery on the school premises.
- Record how and why the decision was made to view the imagery in line with the Record Management Policy and the Child Protection and Safeguarding Policy.
- Make sure that images are viewed by a member of staff of the same sex as the pupil, where appropriate.
- Ensure that, if devices need to be passed on to the police, the device is confiscated, disconnected from Wi-Fi and data and turned off immediately to avoid imagery being accessed remotely; the device will be secured until it can be collected by police.

Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the DSL's professional judgement.

Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.

Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

Following a report of sexting, the following process is followed:

[Note: The process below is recommended in the UK Council for Child Internet Safety's (UKCCIS) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people' guidance. You should amend the text below to suit the process your school follows, in line with any local guidance.]

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

If it is necessary to view the imagery, it will not be copied, printed or shared

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

## **6. Grooming and exploitation**

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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.

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.

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**

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

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Code of Conduct for Adults and Anti-Bullying Policy.

### **Child sexual exploitation (CSE) and child criminal exploitation (CCE)**

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

### **Radicalisation**

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

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

Where staff have a concern about a pupil or another member of staff relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

## **7. Mental health**

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that

training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

## **8. Online hoaxes and harmful online challenges**

For the purposes of this policy, an “**online hoax**” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “**harmful online challenges**” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

The DSL ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content.

The DSL will work with the **SENCO** to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes, e.g. by displaying posters.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.

- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

## 9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

## **10. Online safety training for staff**

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

Online safety training for staff is updated annually and is delivered in line with advice from the local safeguarding partners.

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

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.

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.

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

Staff are required to adhere to the Code of Conduct for Adults at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns.

The DSL acts as the first point of contact for staff requiring advice about online safety.

## **11. Online safety and the curriculum**

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

- Relationships and health education
- PSHE



- Computing

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

- 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. 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
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate
- Knowledge and behaviours that are covered in the government's online media literacy strategy

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 4](#) of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will 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?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will 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 will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be 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.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

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 the Child Protection and Safeguarding Policy.

## **12. Use of technology in the classroom**

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

## **13. Use of smart technology**

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the schools Staff Acceptable use Agreement and Code of Conduct.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

## 14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be 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
- Website information
- Newsletters

Parents will be sent a copy of 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.

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

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

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

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

## **15. Internet access**

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the **academy office**.

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

## **16. Filtering and monitoring online activity**

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be 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. ICT technicians will undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

## **17. Network security**

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a **regular** basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in **class, year or key stage** and above are provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after **90** days, after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

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

Full details of the school's network security measures can be found in the Cyber-security Policy.

## **18. Emails**

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

## **19. Generative artificial intelligence (AI)**

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

## **20. Social networking**

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff can use personal social media during break and lunchtimes in the staffroom and rooms that children do not access;

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

Staff receive annual updates on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will disclose this to the **DSL and headteacher** and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

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

Concerns regarding the online conduct of any member of the school community on social media are reported to the headteacher and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Code of Conduct for Adults and Behaviour Management Policy.

Use on behalf of the school

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

Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

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

## **21. The Academy website**

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the Mobile Phone and Photography Policy are met.

## **22. Use of devices**

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

Use of personal devices/mobile phones is permitted at the academy; however, this is strictly regulated and must be done in accordance with this policy. To minimise any risks, all personal mobiles must not be used where children are present.

Any personal electronic device that is brought into school is the responsibility of the user and must be stored securely, inaccessible to children.

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

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Confidential Reporting Policy.

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 headteacher will inform the police and action will be taken in line with the Confidential Reporting Policy.

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

If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office.

The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Pupils' devices, if found on school premises, can be searched, screened and confiscated in accordance with the latest safeguarding guidance.

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.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

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

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

All school-owned devices are password protected

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.

ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.



Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

### **23. Remote learning**

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

### **24. Monitoring and review**

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct **half-termly** light-touch reviews of this policy to evaluate its effectiveness.

The Directors' board, headteacher and DSL will review this policy in full on an **annual** basis and following any online safety incidents.

The policy was approved by the Directors' Board on \_\_\_\_\_. The next scheduled review date for this policy is **summer term 2024**.

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

Appendix 1: Online Safety Rules and Consent

**Online-Safety Rules**

***All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.***

***Pupil:***

***Year:***

**Pupil's Agreement**

- I have read and I understand the academy Online-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

***Signed:***

***Date:***

**Parent's Consent for Web Publication of Work**

I agree that my son/daughter's work may be electronically published.

**Parent's Consent for Internet Access**

I have read and understood the academy online-safety rules and give permission for my son / daughter to access the Internet. I understand that the academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the academy cannot be held responsible for the content of materials accessed through the Internet. I agree that neither The Societas Trust nor the Academy are liable for any damages arising from use of the Internet facilities.

***Signed:***

***Date:***

***Please print name:***

Please complete, sign and return to your child's class teacher

Appendix 2: Online Safety Posters - Key Stage 1

**Think then Click**

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



B. Stoneham & J. Barrett



## Online Safety Posters - Key Stage 2

### Think then Click

#### Online-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.



## Appendix 3

### Staff Acceptable Use Agreement / Code of conduct



Computing and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of Computing. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with ....., Academy Online-Safety leader.

- I will only use the academy's 's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the computing system security and not disclose any passwords provided to me by the academy or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any academy business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the academy premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal. Images of pupils will only be taken and used for professional purposes and will not be distributed outside the academy network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the academy's Online-Safety policy and help pupils to be safe and responsible in their use of Computing and related technologies.

#### User Signature

I agree to follow this code of conduct and to support the safe use of Computing throughout the academy

Signature \_\_\_\_\_

Date \_\_\_\_\_

Full Name \_\_\_\_

## Online harms and risks – curriculum coverage

[The table below contains information from the DfE’s ‘Teaching online safety in schools’ guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.]

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
<b>How to navigate the internet and manage information</b>		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That age verification exists and why some online platforms ask users to verify their age</li> <li>• Why age restrictions exist</li> <li>• That content that requires age verification can be damaging to under-age consumers</li> <li>• What the age of digital consent is (13 for most platforms) and why it is important</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Health education</li> <li>• Computing</li> </ul>
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What a digital footprint is, how it develops and how it can affect pupils’ futures</li> <li>• How cookies work</li> <li>• How content can be shared, tagged and traced</li> <li>• How difficult it is to remove something once it has been shared online</li> <li>• What is illegal online, e.g. youth-produced sexual imagery (sexting)</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> <li>• Misinformation and being aware that false and misleading information can be shared inadvertently</li> <li>• Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs</li> <li>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons</li> <li>• 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</li> <li>• How to measure and check authenticity online</li> <li>• The potential consequences of sharing information that may not be true</li> </ul>	<ul style="list-style-type: none"> <li>• Relationships and health education</li> <li>• Computing</li> </ul>
<p>Fake websites and scam emails</p>	<p>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 will include the following:</p> <ul style="list-style-type: none"> <li>• How to recognise fake URLs and websites</li> <li>• What secure markings on websites are and how to assess the sources of emails</li> <li>• The risks of entering information to a website which is not secure</li> <li>• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email</li> <li>• Who pupils should go to for support</li> <li>• The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
<p>Online fraud</p>	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What identity fraud, scams and phishing are</li> <li>• That online fraud can be highly sophisticated and that anyone can be a victim</li> <li>• How to protect yourself and others against different types of online fraud</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>

	<ul style="list-style-type: none"> <li>• How to identify 'money mule' schemes and recruiters</li> <li>• The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal</li> <li>• The risk of sharing personal information that could be used by fraudsters</li> <li>• That children are sometimes targeted to access adults' data</li> <li>• What 'good' companies will and will not do when it comes to personal details</li> <li>• How to report fraud, phishing attempts, suspicious websites and adverts</li> </ul>	
<p>Password phishing</p>	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them</li> <li>• How to recognise phishing scams</li> <li>• The importance of online security to protect against viruses that are designed to gain access to password information</li> <li>• What to do when a password is compromised or thought to be compromised</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
<p>Personal data</p>	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How cookies work</li> <li>• How data is farmed from sources which look neutral</li> <li>• How and why personal data is shared by online companies</li> <li>• How pupils can protect themselves and that acting quickly is essential when something happens</li> <li>• The rights children have with regards to their data</li> <li>• How to limit the data companies can gather</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>



<p>Persuasive design</p>	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue</li> <li>• How notifications are used to pull users back online</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Health education</li> <li>• Computing</li> </ul>
<p>Privacy settings</p>	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to find information about privacy settings on various sites, apps, devices and platforms</li> <li>• That privacy settings have limitations</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
<p>Targeting of online content</p>	<p>Much of the information seen online is a result of some form of targeting. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• How the targeting is done</li> <li>• The concept of clickbait and how companies can use it to draw people to their sites and services</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
<p><b>How to stay safe online</b></p>		
<p>Online abuse</p>	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation</li> <li>• When online abuse can become illegal</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>

	<ul style="list-style-type: none"> <li>• How to respond to online abuse and how to access support</li> <li>• How to respond when the abuse is anonymous</li> <li>• The potential implications of online abuse</li> <li>• What acceptable and unacceptable online behaviours look like</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>
Radicalisation	<p>Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to recognise extremist behaviour and content online</li> <li>• Which actions could be identified as criminal activity</li> <li>• Techniques used for persuasion</li> <li>• How to access support from trusted individuals and organisations</li> </ul>	All areas of the curriculum
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal</li> <li>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why</li> <li>• That it is okay to say no and to not take part in a challenge</li> <li>• How and where to go for help</li> <li>• The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> </ul>
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That online content (sometimes gang related) can glamorise the possession of weapons and drugs</li> <li>• That to intentionally encourage or assist in an offence is also a criminal offence</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> </ul>

	<ul style="list-style-type: none"> <li>• How and where to get help if they are worried about involvement in violence</li> </ul>	
Fake profiles	<p>Not everyone online is who they say they are. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'</li> <li>• How to look out for fake profiles</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Boundaries in friendships with peers, in families, and with others</li> <li>• Key indicators of grooming behaviour</li> <li>• The importance of disengaging from contact with suspected grooming and telling a trusted adult</li> <li>• How and where to report grooming both in school and to the police</li> </ul> <p>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.</p>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> </ul>
Livestreaming	<p>Livestreaming (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. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content</li> <li>• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream</li> <li>• That pupils should not feel pressured to do something online that they would not do offline</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>

	<ul style="list-style-type: none"> <li>• The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next</li> <li>• The risks of grooming</li> </ul>	
Pornography	<p>Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That pornography is not an accurate portrayal of adult sexual relationships</li> <li>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour</li> <li>• That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with</li> <li>• How to identify indicators of risk and unsafe communications</li> <li>• The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before</li> <li>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Computing</li> </ul>
<b>Wellbeing</b>		
Impact on confidence (including body confidence)	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• The issue of using image filters and digital enhancement</li> <li>• The role of social media influencers, including that they are paid to influence the behaviour of their followers</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>

	<ul style="list-style-type: none"> <li>• That 'easy money' lifestyles and offers may be too good to be true</li> <li>• The issue of photo manipulation, including why people do it and how to look out for it</li> </ul>	
Impact on quality of life, physical and mental health and relationships	<p>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. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)</li> <li>• How to consider quality vs. quantity of online activity</li> <li>• The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out</li> <li>• That time spent online gives users less time to do other activities, which can lead some users to become physically inactive</li> <li>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues</li> <li>• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support</li> <li>• Where to get help</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Health education</li> </ul>
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> </ul>
Reputational damage	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Strategies for positive use</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> <li>• How to build a professional online profile</li> </ul>	<ul style="list-style-type: none"> <li>• RSHE</li> </ul>
<p>Suicide, self-harm and eating disorders</p>	<p>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.</p>	