Prince Henry's Grammar School
COLLABORATIVE LEARNING TRUST

Online Safety Policy

Approved:	June 2025
Review Period:	Annually
Review Date:	June 2026

Contents

Statement of intent

Prince Henry's Grammar School understands that using online services is an important aspect of raising educational standards, promoting student 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 students 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 students 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 students. Please see the Computing Facilities Guidance and Acceptable Use Policy for further measures that are in place to keep staff safe online.

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 (2024) 'Keeping children safe 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'
- DfE (2023) 'Teaching online safety in school'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Computing Facilities Guidance and Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- PSHE and Citizenship Policy
- Relationships, Sex and Health Education Policy
- Staff Code of Conduct
- Positive Discipline (PD) Behaviour and Safety Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- iPad User Agreement (Student)

2. Roles and responsibilities

The Local Governing Committee (LGC) is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- 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.
- 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 is 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.

- Ensuring staff receive up-to-date online safety training and as part of their induction.
- Ensuring online safety practices are audited and evaluated.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is 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.
- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting 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.
- Review this policy on an annual basis.

ICT technicians are 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 DSL/Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members 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.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns on CPOMS.

Students are responsible for:

- Adhering to this online safety policy 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 to any member of staff or by using the Speak Up button on the school SharePoint.

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

- Staff receive training
- Staff receive email updates regarding online safety information, guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of online safety

Handling online safety concerns

Any disclosures made by students 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 **Safeguarding and Child Protection Policy.**

Concerns regarding a staff member's online behaviour are dealt with in accordance with the **Staff Code of Conduct, Disciplinary Policy and Procedure, and Safeguarding and Child Protection Policy.**

Where there is a concern that illegal activity has taken place, a member of the safeguarding team will contact the Police.

The school avoids unnecessarily criminalising students, 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 student 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 Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded on CPOMS.

4. Cyberbullying

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against students 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

Students 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 and off and online, and will remain aware that students 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
- Downblousing, i.e. taking a picture down a person's top without consent
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds 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 are reported to the safeguarding team, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

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 students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.
- The student 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 students 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.
- 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.

Concerns relating to child sexual exploitation (CSE) and child criminal exploitation (CCE) and radicalisation should be reported to the safeguarding team through CPOMS as set out in the Safeguarding and Child Protection policy.

6. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a student'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 student is suffering from challenges in their mental health.

7. Harmful online challenges

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to a member of the safeguarding team immediately through CPOMS.

The safeguarding team 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 students, 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.

The DSL and headteacher will determine a proportionate response which is in line with school policy and national guidance.

Where the safeguarding team's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant students, e.g. those within a particular age range that is directly affected or even to individual children 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 students' exposure to the risk is considered and mitigated as far as possible.

8. 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 students 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 student'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 students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology.

9. Online safety and the curriculum

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

- PSHE & Citizenship
- Computing

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

Students 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 students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour (including cyberbullying)
- 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

The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these students receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. 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 students?
- Are they appropriate for students' developmental stage?

Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse. If a staff member is concerned about anything students disclose during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection policy.

10. Use of technology in the classroom

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource.

Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

11. Use of smart technology (iPads and mobile phones)

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.

Students will be educated on the acceptable and appropriate use of personal devices.

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

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.

Where there is a significant problem with the misuse of smart technology among students, the school will discipline those involved in line with the school's Positive Discipline (PD) Behaviour and Safety Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

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

12. Educating parents

The school works in partnership with parents to ensure students stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children in an annual parent event hosted at the school. Parents are 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.

The school has a dedicated E-Learning and Online Safety section on the website which can be used as a resource bank for parents.

13. Internet access

Staff and other members of the school community are only granted access to the school's internet network once they have completed Cyber Awareness training and signed the

Acceptable Use Agreement. Students will cover Cyber Safety within the Curriculum so are simply expected to acknowledge and accept the Acceptable Use Agreement within Arbor.

All members of the school community are 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.

14. Filtering and monitoring online activity

The Local Governing Committee (LGC) ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The DSL and ICT technicians undertake a termly review to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks.

Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Positive Discipline (PD) Behaviour and Safety 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 Police.

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

15. Network security

Technical security features, such as anti-virus software (Sophos), are kept up-to-date and managed by the central CLT IT staff. Firewalls are switched on at all times. IT staff review the central monitoring dashboards for alerts on at least a weekly basis to ensure they are running correctly, and to carry out any required action/updates.

Staff and students are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to IT Support.

All members of staff have their own unique usernames and private passwords to access the school's systems. Staff members and students are responsible for keeping their passwords

private. In line with the most recent guidance from the National Cyber Security Centre, we insist that all passwords should meet the criteria below:

- Must include three random, unrelated words (e.g. penciltrainfish but NOT twothreefour).
- Must be at least 12 characters long.
- *May* include a mixture of uppercase and lowercase letters, numbers, and special characters (e.g. PencilTrainFish3?).
- Must not be identical or substantially similar to any previous passwords.
- Must not be related to one's job or personal life (e.g. a spouse's name or fragments of an address).
- Must be committed to memory and not written down.
- Should only be changed when there is a data breach, or whenever a member of staff suspects that a password has become known to another person.

Due to the increased complexity of these passwords, they will not expire.

Please the see Computing Facilities Guidance and Acceptable Use policy for further information.

Users must inform IT Support if they forget their login details. IT staff will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not 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 (staff) or Year Manager (students) is informed and decides the necessary action to take. Where there is an inherent risk, or potential risk, to school's systems and services, or for unauthorised access to data, IT staff may disable that person's network access with immediate effect.

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

16. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, and Acceptable Use Agreement. For information pertaining to staff and emails please see the Computing Facilities Guidance and Acceptable Use Policy.

Students are given approved school email accounts. Prior to being authorised to use the email system, students must agree to the terms of the Acceptable Use Agreement by confirming that they have read and understood the agreement. Personal email accounts are not permitted to be used on the school site.

Students are 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. Information is provided as part of the Computing curriculum to students to educate them about:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

17. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Students are not permitted to use social media for personal use during lesson time.

For information pertaining to staff and social networking please see the Computing Facilities Guidance and Acceptable Use Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy.

18. Use of devices

School-owned devices

Every student is issued with an iPad when they arrive at the school.

School-owned devices are used in accordance with the Acceptable Use Agreement. All school-owned devices are password protected and they are fitted with tracking software to ensure they can be retrieved if lost or stolen. 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 regularly to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the user. Students from year 7-11 are not permitted to use mobile phones their personal devices at any point when they are on the school site. If a student needs to contact their parents during the school day, they must seek permission from a member of staff. Sixth form students do have permission to use their mobile phone during social times in the Quad.

Where a student uses accessibility features on a personal device to help them access education, e.g. where a student who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL. Please see our Mobile Phone Policy for further detail.

19. Remote learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

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.
- Direct parents to useful resources to help them keep their children safe online.

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

Appendix A: 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. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • 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 areas: • PSHE and Citizenship education • (including Health education) • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect students' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and

	• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	Health education)
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What students should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who students should go to for support	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so	This risk or harm is covered in the

	they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How students can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • 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 • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that	This risk or harm is covered in the

	can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	following curriculum areas: • PSHE and Citizenship education • (including Health education) • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • 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 • How the targeting is done • 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 areas: • PSHE and Citizenship education • (including Health education) • Computing
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. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE and Health education) • Computing

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

Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE)
Livestreaming	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 includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if students would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That students should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including Health Education)

	• The risks of grooming	
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • 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 areas: • PSHE and Citizenship education • (including RSE)
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE) • Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education

	• The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	• (including Health Education)
Impact on 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. Teaching includes the following: • How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for students 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 or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including Health Education)
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • 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 or curated lives • 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 areas: • PSHE and Citizenship education • (including RSE and Health Education)

Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum areas: • PSHE and Citizenship education • (including RSE)
Suicide, self-harm and eating disorders	Students 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 students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	• PSHE and Citizenship education