THE BEACON

Online Safety Policy

Review cycle:	Every year
Review by:	SMT, G(Ed)
Last Governor Approval:	Spring 2026
Next Governor Approval:	Spring 2027

Policies Linked to:

- Anti-Bullying Policy
- Behaviour Policy
- Staff Induction Policy
- Health & Safety Policy
- Risk Assessment Policy
- Staff Employment Manual
- Pupil Acceptable Use Policy
- IT Acceptable Use Policy
- SEMH Policy
- Safegaurding & Child Protection Policy

This document also appears on:

- Staff Intranet

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. Staff training
11. Online Safety and the curriculum
12. Educating parents
13. Classroom use
14. Internet access
15. Filtering and monitoring online activity
16. Network security
17. Emails
18. Social networking
19. The school website
20. Use of school-owned devices
21. Use of personal devices
22. EYFS (Early Years Foundation Stage)
23. Responding to specific online safety concerns
24. Remote learning
25. Monitoring and review

Appendices

Appendix 1 – Dealing with Incidents of Misuse

Appendix 2 – Online harms and risks – curriculum coverage

Statement of intent

The Beacon 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, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **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 General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2025) ‘Keeping children safe in education 2025’
- 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 (January 2023) ‘Teaching online safety in school’
- DfE (July 2023) ‘Searching, screening and confiscation’
- National Cyber Security Centre (2017) ‘Cyber Security: Small Business Guide’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- UK Council for Child Internet Safety (2017) ‘Sexting in schools and colleges: Responding to incidents and safeguarding young people’

This policy operates in conjunction with the following school policies:

- Photography Social Media Policy
- Allegations of Abuse Against Staff Policy
- Low-Level Safeguarding Concerns Policy
- Child on Child Abuse Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy

- Data Protection Policy
- Pupil Remote Learning Guidance
- Technology Acceptable Use Agreement for Pupils
- SEMH Policy

2. Staff Roles and responsibilities

The governing board 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.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- The IT Governor is Dipen Thaker

The Headmaster is responsible for:

Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

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.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- 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.

- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, IT Department, and Head of Computing.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a co-ordinated 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.
- Working closely with the police during police investigations
- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils 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.
- Reporting to the governing board about online safety on a termly basis.
- Working with the governing board to update this policy on an annual basis.
- Understand the school's monitoring and filtering systems.
- Working with the ICT Department to ensure that all students, staff and parents are aware of the school's monitoring and filtering systems.
- Working with the ICT Department to annually review the school's monitoring and filtering systems

ICT department are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Working conjunction with the Senior Management Team to implement appropriate security measures
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL to annually review the filtering and monitoring systems.

All staff members are responsible for:

- Taking responsibility for the security of IT 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.
- Having an awareness of the school's filtering and monitoring systems.

Pupils are responsible for:

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

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, the Head of Computing, and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils’ safety online.

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

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online
- Online Safety (Including Monitoring & Filtering) is a standing agenda item on the Safeguarding Team’s weekly meeting.

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 pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

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 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 still be 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 and appropriate support provided to the victim.

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. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and 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, ICT technicians, and Head of Computing, 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 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
- 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 and 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
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

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.

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 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 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 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, including the following:

- The pupil 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 pupil 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 pupil 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 pupil feel 'special', particularly if the person they are talking to is older.
- 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.
- 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.

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.

Where staff have a concern about a pupil 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

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, 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 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.

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.

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.

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, 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 pupils, 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 pupils' exposure to the risk is considered and mitigated as far as possible.

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, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Staff training

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 three local safeguarding partners.

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

The DSL and 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 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 including recognising the additional risks that pupils with SEND face online and offer them support to stay safe online. All staff are made aware of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media. Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

11. Online Safety and the curriculum

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

- SAS/RSE
- PSHE/Citizenship
- Computing

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.

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

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

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

The DSL is involved with the development of the school's online safety curriculum.

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

External resources are reviewed prior to use, 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 DSL or Deputy Head (Academic and Digital) 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 teacher considers the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel 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 sections 15 and 16 of this 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 sections 15 and 16 of this policy.

12. Use of Technology in the Classroom

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

- Computers
- Laptops (School and personal)
- 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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised and their devices are monitored 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 Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

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. As a consequence, pupils are not permitted to use a mobile phone whilst on school premises, during school time or on school transport.

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 pupils, the school will discipline those involved in line with the school's Behavioural 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 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 4C's (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 works in partnership with parents to ensure pupils 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. Parental awareness is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- E-Safety Resources on the Parent Portal

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.

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.

15. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

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.

16. Filtering and monitoring online activity

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The IT Department ensure 'over blocking' does not lead to unreasonable restriction as to what pupils can be taught with regards to online teaching and safeguarding.

IT Department undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the IT Department

Any changes made to the system are recorded by IT Department.

Reports of inappropriate websites or materials are made to a member of the IT department immediately, who investigates the matter and makes any necessary changes.

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

If a pupil has deliberately breached the filtering system, they will be sanctioned 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 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 sections 15 and 16 of this policy.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by IT Department and the Network Manager.

Firewalls are switched on at all times.

Firewall is updated when required – that applies to both firewall rules that control the traffic and the actual firmware updates.

Staff and pupils will not download unapproved software or open unfamiliar email attachments.

Staff members and pupils report all malware and virus attacks to IT Department.

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

Pupils in Year 4 and above are provided with their own unique username and private passwords. Pupils in Year 3 share a common password.

Staff members and pupils are responsible for keeping their passwords private.

Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

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

Users inform IT Department if they forget their login details, who will arrange for the user to access the systems under different login details.

If a user is found to be sharing their login details or otherwise mistreating the password system, the Deputy Head (Academic and Digital) is informed and decides the necessary action to take.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Policy.

Staff and pupils are given approved school email accounts and are only 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 relevant acceptable use agreement.

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

Spam should be blocked automatically by our systems. Staff can report and spam emails that they have received into their regular inboxes.

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

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

19. Social networking

Personal use

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; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

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

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.

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 DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

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

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

Staff members must be authorised by the Headmaster 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 Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

20. The school website

The Head of Marketing is 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 Photography and Social Media Policy are met.

21. Use of school-owned devices

Teaching Staff members are issued with a laptop to assist with their work.Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. i-pads or chrome books to use during lessons.

All mobile school-owned devices 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.

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

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

22. Use of staff and pupil personal devices

Personal devices are used in accordance with the IT Acceptable Use Policy for Personal Devices (Staff and Visitors).

Any personal electronic device that is brought into school is the responsibility of the user.

All students in Year 7 are issued with a personal device (laptop).

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency or if prompted to approve a 2-factor authentication sign-in to their account.

Where no school devices are available, staff members are permitted to use their personal devices to take photos or videos of pupils in educational activities as long as the photographs are downloaded onto the school server and the photos are removed from the personal device within 24 hours. This does not apply to EYFS staff who must not use their personal devices under any circumstance to photograph the pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Safeguarding and Child Protection 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 Headmaster will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

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.

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

Pupils should not use their mobile phone whilst on school premises or during school time.

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

Pupils' devices can be searched, screened and confiscated.

23. Early Years Foundation Stage (EYFS)

The Use of Cameras

Under the General Data Protection Regulation (2018) photographs and videos of adults and children are regarded as personal data and must be respected as such.

Safe practice is communicated to adults within the setting. We ask for individual permissions for photographs and video recordings for a range of purposes including use in the child's learning journey.

We ensure parents understand that where their child is also on another child's photograph, but not as the primary person, that may be used in another child's learning journey.

If a parent does not consent to one or more of these uses, we find alternative ways of recording their child's play or learning.

Parents are not permitted to use any recording device or camera (including those on mobile phones) on the setting premises without the prior consent of the Head of Pre-Prep.

The setting;

- Has *written* consent from parents for photographs of their children to be taken and used. Verbal consent is not considered acceptable.

- Has *written* consent from adults employed in the setting for their photograph to be taken or used

- Consent includes permission to store / use images once a child has left the setting-
- e.g. for brochures, displays etc. Parents are informed of the timescale for which images will be retained.

- Permission is obtained every year.

- Asks parents to inform the setting immediately if they wish permission to be rescinded.

- Parents are informed of the purposes for which images may be taken and used e.g.displays, website, brochures, learning journeys and portfolios,

- Images may be displayed in public areas around the setting to demonstrate activities and learning.

- If trainees / students not directly employed by the setting wish children's images to be included in portfolios, parental permission will be sought

- The press has special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph. The setting will always inform parents of this and obtain written permission from parents for this.

Taking Photographs / Video

The staff designated to take images of children are their class teachers, teaching assistants, marketing team staff and Head of Pre-Prep.

Photographs and videos are only taken using equipment provided by the setting.

When taking photographs/ video children's right to refuse to be photographed is respected

Photographs will never show children who are distressed

When taking images care will be taken to ensure that certain children are not continually favoured

Subjects are appropriately dressed and not participating in activities that could be misinterpreted. This would include for example considering the angle of shots for children engaged in PE activities.

Certain areas of the setting are 'off limits' for taking photographs, e.g toilets, changing rooms, cubicles etc.

Close up shots are avoided as these may be considered intrusive.

Shots will preferably include a background context and show children in group situations.

Parents Taking Photographs / Video

Under the General Data Protection Regulation (2018), parents are entitled to take photographs of *their own* children on the provision that the images are for *their own* use, e.g. at a School production. Any other purpose is a potential breach of Data Protection legislation.

Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults

Parents are reminded, preferably in writing, that publishing images which include children other than their own or other adults on Social Network sites is unacceptable, unless specific permission has been obtained from the subjects

The setting has a request form that 'allows' parents to use cameras at a specified time / in a specified area for a particular purpose

Parents are encouraged to be considerate when taking photographs, e.g. Not obscuring the view of others or being intrusive

Storage of Photographs / Video

The setting ensures photographs are securely stored and not removed from the setting

If images are stored on USB memory sticks, they are encrypted or password protected

Only authorised staff have access to photographs / videos stored on our equipment

Authorised staff are responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed

Authorised staff ensure images are disposed of should a parent withdraw permission.

Publication of Photographs / Videos

Consent is obtained from parents for publication of children's images, e.g. on a website.

Photographs are only published online to secure sites.

When publishing photographs care is taken over the choice of images
to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse,

Full names and / or other personal information never accompany published images on external media outlets.

The setting takes care to ensure that children's images are not displayed on insecure sites e.g. personal Social Networking Sites.

Staff are aware that full names and personal details will not be used on
digital media, particularly in association with photographs.

Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites **CCTV, Video Conferencing and Webcams**

Parents are informed if CCTV or webcams are in use in the setting.

If CCTV or webcams are to be used the cameras will not overlook sensitive areas.

24. Responding to specific online safety concerns

The school will respond to all reports of online child-on-child abuse or sexual harassment whether or not the incident took place on the school premises or using school-owned equipment.

Concerns of online abuse or harassment are to be reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Information about the school's full response to incidents of online child-on-child abuse can be found in 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.

Following a report of sexting, 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
- 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 headmaster 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.

Online abuse and exploitation

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. Staff Code of Conduct, Anti-Bullying Policy and Adult Code of Conduct.

Online radicalisation and extremism

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

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

25. Monitoring and review

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

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

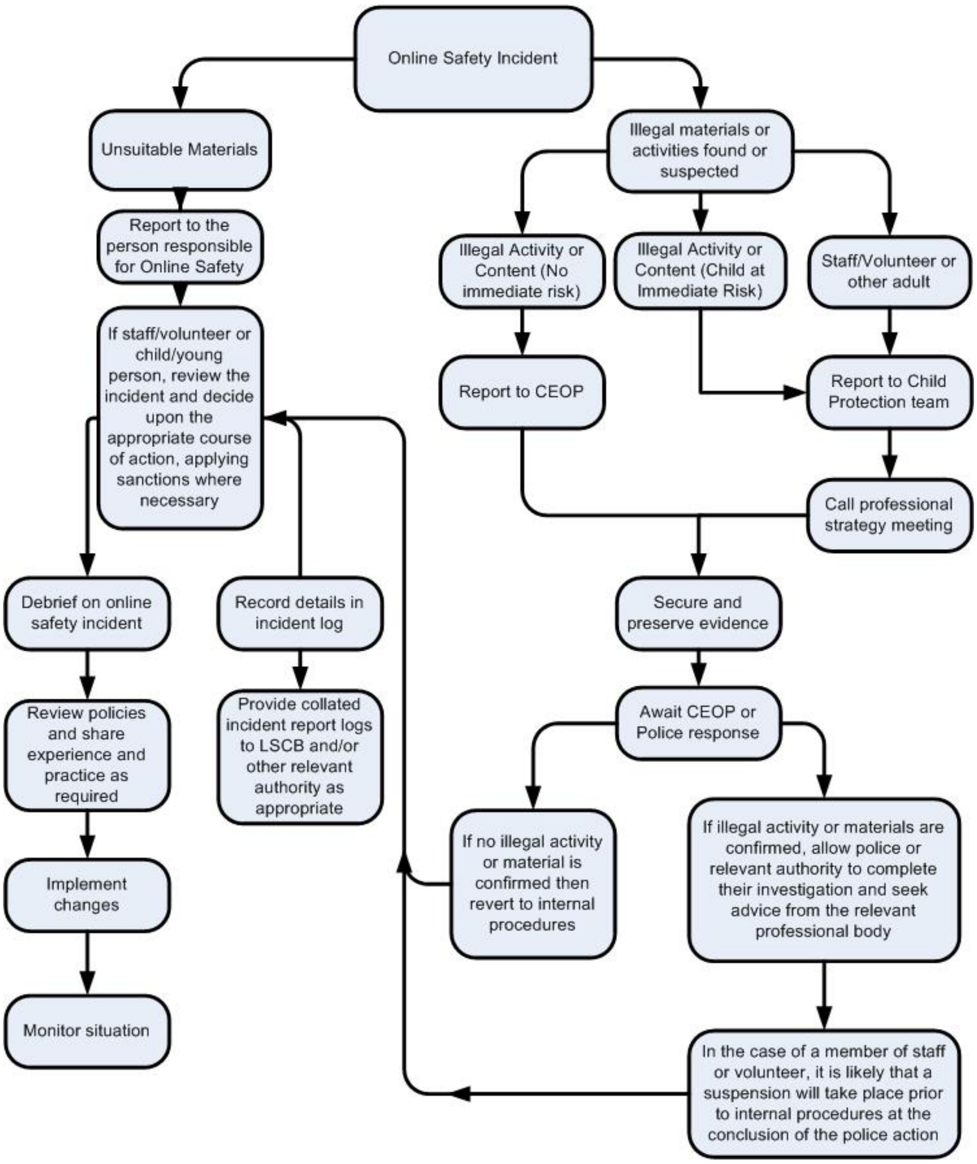
Any changes made to this policy are communicated to all members of the school community.

Appendix 1 Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Beacon policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

Current threat levels are constantly monitored and children are advised accordingly.

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).

Police involvement and/or action should take place if content being reviewed includes images of Child abuse then the monitoring be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Beacon and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 2: 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 area(s): • Computing curriculum
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 pupils' 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 area(s): • Relationships education • RSE • Computing curriculum
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 area(s): • Relationships education

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

	• 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	• Relationships education • Computing curriculum
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 pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE • Computing curriculum
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 – 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 area(s): • Computing curriculum
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Targeting of online content	Much of the information seen online is a result of some form of targeting.	This risk or harm is covered in the

	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	following curriculum area(s): • Health education • Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. 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 area(s): • Relationships education • RSE • Computing curriculum • Citizenship
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges	This risk or harm is covered in the following curriculum area(s): • Relationships education

Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines). Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE

Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out live streaming 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 pupils 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 pupils 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 • The risks of grooming	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
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 area(s): • 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:	This risk or harm is covered in the following curriculum area(s):

	• 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 pupils 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	• Relationships education • RSE • Computing curriculum
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 • 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	This risk or harm is covered in the following curriculum area(s): • 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 pupils 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 pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or 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	This risk or harm is covered in the following curriculum area(s): • Health education

	• 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 • Where to get help	
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/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 area(s): • Relationships 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 area(s): • RSE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	