MAHARISHI SCHOOL

Online Safety Policy

February 2026

Start Date: February 2026

Review Date: February 2027

Signed by:

Headteacher	Lisa Edwards	Date	Feb 26
Chair of Governors	Ian Birnbaum	Date	Feb 26

Contents:

Statement of intent

Maharishi School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

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

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

1. Legal framework

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

Online Safety Act 2023

Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

Data Protection Act 2018

DfE 'Filtering and monitoring standards for schools and colleges'

DfE ‘Harmful online challenges and online hoaxes’

DfE ‘Keeping children safe in education 2025’

DfE ‘Teaching online safety in school’

DfE ‘Searching, screening and confiscation’

DfE ‘Generative artificial intelligence in education’

Department for Digital, Culture, Media and Sport and UK Council for Internet Safety ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’

UK Council for Child Internet Safety ‘Education for a Connected World – 2020 edition’

National Cyber Security Centre ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

Social Media Policy

Allegations of Abuse Against Staff Policy

ICT Acceptable Use Agreement

Cybersecurity Policy

Child-on-Child Abuse Policy

Anti-Bullying Policy

Staff Code of Conduct

Enabling Good Behaviour Policy

Disciplinary Policy and Procedures

Data Protection Policy

Confidentiality Policy

Photography and Images Policy

Prevent Duty Policy

Remote Education Policy

2. Roles and responsibilities

The governing body will be responsible for:

• Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

• Ensuring the Designate Safeguarding Lead's (DSL) remit covers online safety.

• Reviewing this policy on an annual basis.

• Ensuring their own knowledge of online safety issues is up-to-date.

• Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

• Ensuring that there are appropriate filtering and monitoring systems in place.

• Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

• Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

• Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

• Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher will be responsible for:

• Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

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

• Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

• Ensuring online safety practices are audited and evaluated.

• Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

• Working with the DSL and ICT support team to conduct half-termly light-touch reviews of this policy.

• Working with the DSL and governing body to update this policy on an annual basis.

• Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.

• Appointing an SLT digital lead in line with the Cyber-security Policy.

The DSL will be responsible for:

• Taking the lead responsibility for online safety in the school.

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

• Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT support team.

• Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

• Ensuring safeguarding is considered in the school's approach to remote learning.

• Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

• Understanding the filtering and monitoring processes in place at the school.

• Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

• 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 body about online safety on a termly basis.

• Working with the headteacher and ICT support team to conduct termly

light-touch reviews of this policy.

• Working with the headteacher and governing body to update this policy on an annual basis.

ICT support team will be responsible for:

• Providing technical support in the development and implementation of the school's online safety policies and procedures.

• Implementing appropriate security measures as directed by the headteacher and/or Business Support Team.

• Ensuring that the school's filtering and monitoring systems are updated as appropriate.

• Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

All staff members will be responsible for:

• Taking responsibility for the security of ICT systems and electronic data they use or have access to.

• Modelling good online behaviours.

• Maintaining a professional level of conduct in their personal use of technology.

• Having an awareness of online safety issues.

• Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.

• Reporting concerns in line with the school's reporting procedure.

• Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

• Adhering to the Acceptable Use Agreement and other relevant policies.

• Seeking help from school staff if they are concerned about something they or a peer have experienced online.

• Reporting online safety incidents and concerns in line with the procedures within this policy

3. Managing Online Safety

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

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

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

Regular training for staff; online safety integrated into learning throughout the curriculum; assemblies and PSHE lessons conducted on the topic of remaining safe online

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 Safeguarding and Child Protection Policy and/or the Child-on-Child Abuse Policy. Pupils, whether victims or perpetrators, will be supported accordingly.

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

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

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

the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour will be reported to the headteacher, who will decide on the best course of action in line with the relevant policies. If the concern is about the headteacher, it will be reported to the Chair of Governors.

Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate concerns in accordance with relevant policies depending on their nature, e.g. Enabling Good Behaviour Policy, Safeguarding and Child Protection Policy, Child-on-Child Abuse Policy.

Where there is a concern that illegal activity has taken place, the headteacher or DSL will contact the police.

The school will avoid 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.

4. Cyberbullying

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

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

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

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they

occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

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

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

Threatening, facilitating or encouraging sexual violence; upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks; sexualised online bullying, e.g. sexual jokes or taunts; unwanted and unsolicited sexual comments and messages; consensual or non-consensual sharing of sexualised imagery; abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff promote a zero-tolerance approach to sexual harassment or abusive behaviour and any attempts to pass such behaviour off as trivial or harmless. Staff are 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 are 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, Child Protection and Safeguarding Policy, and the Social Media Policy.

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

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

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

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including: Being secretive about how they are spending their time online; having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met; having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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. 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 Safeguarding Policy and Child Protection 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 and are 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 Child Protection and Safeguarding Policy and the Prevent Duty Policy.

7. Mental health

Staff are 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 school's unique system of Consciousness-based Education places emphasis on the wellbeing of its pupils and staff: Why Maharishi School Is Unique

The school also has a fully trained Senior Mental Health Lead, a highly qualified Family Support Worker, an Emotional Literacy Support Assistant, a trained Drawing and Talking Therapy practitioner and a staff member trained in offering suicide prevention support.

Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

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

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge

itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

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

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

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

• In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when factchecking the risk of online challenges or hoaxes.

• Not needlessly scaring or distressing pupils.

• Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.

• Proportional to the actual or perceived risk.

• Helpful to the pupils who are, or are perceived to be, at risk.

• Appropriate for the relevant pupils' age and developmental stage.

• Supportive.

• In line with the Child Protection and Safeguarding Policy.

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

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of an online 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.

10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. Staff are made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that abuse can take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider

curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online safety and the curriculum

Regular practice of TM, and understanding of CbIDS, provides a sense of personal stability, providing a strong sense of self. This can act as a barrier between a user and online safety issues. In any unfortunate instances where such experiences have occurred, the practice of TM can help to restore imbalance caused by such stressful experiences.

Online safety is explicitly taught through Personal Social Health Education (PSHE), Relationships and Health Education (RHE)/Relationships, Sex and Health Education and computing. 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 school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, selfharm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and nonconsensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

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

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way

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

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

Technology used during lessons will include chromebooks, including Google Classroom and Gmail. Cameras and mobile phones (secondary phase art/photography lessons) may be used.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource.

Class teachers will ensure that any internet-derived materials are used in line with copyright law. Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

Primary phase pupils are not permitted to bring mobile phones or any other personal technology into school. Secondary phase pupils may bring mobile phones with them to school, however, these devices must be handed in at the start of the school day and can be collected at the end. Issues related to mobile phones are considered under the Mobile Phone Policy.

The school will address concerns related to the misuse of smart technology through assemblies and PSHE lessons, outlining the importance of using smart technology in an appropriate manner.

14. Educating parents

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. Parents' attention will be drawn to issues of concern and useful links for parents via email and the school website. Internet issues will be handled sensitively to inform parents without undue alarm.

15. Internet access

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

16. Filtering and monitoring online activity

The school's ICT network has appropriate filters and monitoring systems in place. Staff will liaise with the Business Support Team (who will liaise with IT support) to ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. Reports of

inappropriate websites or materials will be made to the Business Support Team, the headteacher or deputy heads who will inform IT support immediately, ensuring any necessary changes are made.

The school's network and school-owned devices will be appropriately monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the appropriate policy, determined on a case-by-case basis.

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be made aware of the various ways in which their children may be at risk online.

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

17. Network security

Anti-virus software will be kept up-to-date and managed by the IT support team. Firewalls will be switched on at all times and reviewed at regular intervals. All staff have completed Cyber Awareness training, including the advice not to download unapproved software or open unfamiliar email attachments. Malware and virus attacks will be reported to the IT support team.

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

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

18. Emails

All staff members have a school email account to enable professional communication. This should not be used for personal emails and personal email accounts should not be used for work-related activities.

Pupils have a school email account and may contact staff via this medium to discuss school-related matters.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians via the Business Support Team. The school's monitoring system can detect inappropriate links, malware and profanity within

emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

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

19. Generative artificial intelligence (AI)

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

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

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

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

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

20. Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

21. The school website

The headteacher 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.

22. Use of devices

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

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

23. Remote learning

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

21. Monitoring and review

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

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

The next scheduled review date for this policy is February 2027.

Online harms and risks - curriculum coverage

How to navigate the internet and manage information		
Subject area	Description & teaching content	Curriculum area the harm or risk is covered in
Age restrictions	* 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	PSHE Computing
How content can be used and shared	* 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	PSHE RHE (primary) RSHE (secondary) Computing

	shared online * What is illegal online, e.g. youth-produced sexual imagery (sexting)	
Disinformation, misinformation and hoaxes	* Disinformation and why individuals or groups choose to share false information in order to deliberately deceive * Misinformation and being aware that false and misleading information can be shared inadvertently * Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs * 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	PSHE RHE (primary) RSHE (secondary) Computing

	* How to measure and check authenticity online * The potential consequences of sharing information that may not be true	
Fake websites and scam emails	* 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, or groomed as a result of interacting with a fake website or scam email * Who pupils should go to for support * The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services	PSHE RHE (primary) RSHE (secondary) Computing

	that do not exist	
Online fraud	* What identity fraud, scams and phishing are * That online fraud can be highly sophisticated and that anyone can be a victim * How to protect yourself and others against different types of online fraud * How to identify 'money mule' schemes and recruiters * The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal *The risk of sharing personal information that could be used by fraudsters * That children are sometimes targeted to access adults' data * What 'good' companies will and will not do when it comes to personal details	PSHE Computing

	* How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	* 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	PSHE Computing
Personal data	* 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	PSHE Computing

	something happens * The rights children have with regards to their data * How to limit the data companies can gather	
Persuasive design	* That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue * How notifications are used to pull users back online	PSHE Computing
Privacy settings	* How to find information about privacy settings on various sites, apps, devices and platforms * That privacy settings have limitations	PSHE Computing
Targeting of online content	* How adverts seen at the top of online searches and social media	PSHE Computing

	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	
How to stay safe online		
Online abuse	* The types of online abuse, including sexual harassment, bullying, trolling and intimidation * When online abuse can become illegal * How to respond to online abuse and how to access support * How to respond when the abuse is anonymous * The potential implications of online abuse * What acceptable and unacceptable online behaviours look like	PSHE RHE (primary) RSHE (secondary) Computing

Radicalisation	* How to recognise extremist behaviour and content online * Which actions could be identified as criminal activity * Techniques used for persuasion * How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	* 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	PSHE RHE (primary) RSHE (secondary)
Content which incites	* That online content	PSHE

violence	(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	
Fake profiles	* 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	PSHE RHE (primary) RSHE (secondary) Computing
Grooming	* 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	PSHE RHE (primary) RSHE (secondary)

	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.*	
Live streaming	* What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content * 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 * 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	PSHE RSHE (secondary)

Pornography	* 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, e.g. revenge porn or people trafficked into sex work	RSHE (secondary)
Unsafe communication	* 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	PSHE RHE (primary) RSHE (secondary) Computing

	confidently say no to both friends and strangers online	
Wellbeing		
Impact on confidence (including body confidence)	* 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 * That 'easy money' lifestyles and offers may be too good to be true * The issue of photo manipulation, including why people do it and how to look out for it	PSHE RSHE (secondary)
Impact on quality of life, physical and mental health and relationships	* 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	PSHE

	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 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	* How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	PSHE RHE (primary) RSHE (secondary)

Reputational damage	* Strategies for positive use * How to build a professional online profile	PSHE RSHE (secondary)
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.	PSHE RSHE (secondary)