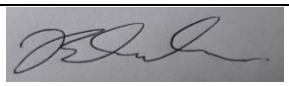
Townhill Junior School

Online Safety Policy

Online Safety Policy			
Date last amended:	4th October 2024	**Approved by:**	Townhill Junior School Full Governing Body
Approval date:	14th October 2024	**Signed:**	 Jo Proctor Chair of Governors
Review Date:	October 2025		

Contents:

Statement of intent

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

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

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

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

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy
- Photography and Images Policy
- Staff ICT and Electronic Devices 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 DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

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

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 the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technician 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.

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 technician.
- 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 technician to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing body to update this policy on an annual basis.

The Online Safety Group are responsible for:

- Linking Online Safety to Computing, PSHE and the wider curriculum
- Engaging pupils directly with the contents of the policy
- Developing a culture of safety online within the school and the wider community

The ICT technician will be responsible for:

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

All staff members will be responsible for:

- Ensuring devices are locked and appropriately stored to ensure sensitive data is not visible or accessible to others
- 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.
- Ensuring vigilance when opening emails and their attachments, with concerns being reported to the DSL or the ICT Technician as appropriate.
- 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, the headteacher and The Online Safety Group where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and governors receive regular training
- 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 termly on the topic of remaining safe online
- Regular updates for parents on new or pertinent online safety issues

Handling online safety concerns

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

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

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

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

Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate concerns with relevant staff members, e.g. the headteacher and ICT technician, and will manage 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. reporting as a crime, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

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

4. Cyberbullying

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

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

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

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

5. Child-on-child sexual abuse and harassment

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

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

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

- 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.

Staff will be aware that it is illegal to view any indecent images of children and will need to take particular care when an incident is reported by a parent, that they ask what any images contain before they view them. Staff will be aware that they should not open email attachments that could contain indecent images. Staff will direct parents to the police if images are believed to contain illegal content.

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

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

6. Grooming and exploitation

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

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

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

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

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

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

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

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

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

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

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

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

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 will ensure 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. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

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

- Relationships and health education
- PSHE
- Citizenship
- Computing

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online

- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

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

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

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

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

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

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

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

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

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

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

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets / IPads
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

13. Use of smart technology

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

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

Inappropriate use of smart technology may include:

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

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

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

14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the start of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

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

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

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

- Parents' evenings
- Newsletters
- Online resources

15. Internet access

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

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

16. Filtering and monitoring online activity

The governing body will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technician will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The ICT technician will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

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

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

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

17. Network security

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

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

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

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

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

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

18. Emails

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

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

Staff members and pupils will be required to block spam and junk mail, and report the matter to the ICT technician. 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. The Online Safety Ambassadors will organise an annual assembly where they explain about staying safe online.

Any cyber-attacks initiated through emails will be managed in line with the School Emergency 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 Networking Policy.

21. The school website

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

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 Acceptable 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.

23. Remote learning

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

24. Monitoring and review

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

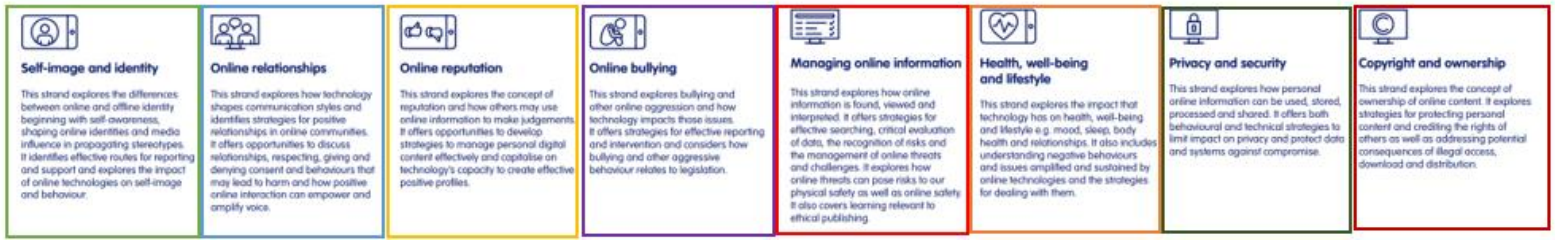
The governing body, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is October 2025.

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

Appendix A: Whole School Online Safety

Through PSHE and our Computing curriculum we cover many aspects of online safety. We use the [Education for a Connected World Framework] to ensure we are covering a wide range on online safety contexts. These are highlighted on this document.



	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
WIDER CURRICULUM	Know How Rules Protect Us whole school assembly		Safer Internet Day – theme in assembly and followed up with class and year group assemblies and activities Tolerance whole school assembly	Respect and Tolerance whole school assembly		
Year 3	**Being Me in My World** **ONLINE RELAITONSHIPS** **Piece 4:** Scenarios around nasty text messages	**Celebrating difference** **ONLINE BULLYING** **Piece 3:** Discussions about what bullying is – can link to cyber bullying. **Piece 4:** Scenarios around watching scary YouTube videos. **Computing**	**Computing** **MANAGING ONLINE INFORMATION** -I can use key phrases in search engines -I can use search technologies effectively	**Healthy Me** **ONLINE RELAITONSHIPS** **HEALTH, WELLBEING AND LIFESTYLE** **Piece 4:** Thinking about when they feel safe or unsafe – could link to situations on the internet.	**Relationships** **ONLINE REPUTATION** **Piece 3:** Keeping myself safe online Children learn and rehearse using strategies for keeping themselves safe online; they also learn who to ask for help if they are worried or concerned about anything online.	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
		MANAGING ONLINE INFORMATION -I can use key phrases in search engines. -I can use search technologies effectively.	**COPYRIGHT AND OWNERSHIP** -When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it -I can demonstrate the use of search tools to find and access online content which can be reused by others	**ONLINE REPUTATION** **Piece 5:** Scenarios explore what to in safe/unsafe situations. One example reference posting something online that they should not be doing. **HEALTH, WELLBEING AND LIFESTYLE** **Piece 6:** Children to create an infographic on how to stay safe. Opportunities for children to talk about how to stay safe on the internet and limit their screen time to improve their health.	**ONLINE BULLYING** **Piece 3:** Keeping myself safe online Children learn and rehearse using strategies for keeping themselves safe online; they also learn who to ask for help if they are worried or concerned about anything online.	
Year 4		**Celebrating Difference** **ONLINE BULLYING** **Piece 3:** Discussion around a story where online bullying has occurred. Children need to think about how it has affected the child and what should be done and what the bystanders should/ should not do.	**Dreams and Goals** **ONLINE REPUTATION** **Piece 2:** Scenarios that get the children to think about how the someone might feel if they didn't get what they wanted and about being resilient. One situation is about someone not getting likes on social media. Children to understand that it isn't the end of the world and	**Healthy Me** **ONLINE RELATIONSHIPS** **ONLINE REPUTATION** **Piece 2:** Discussions around peer pressure. Scenarios around sending rude messages on phones.	**Relationships** **ONLINE RELATIONSHIPS** **ONLINE REPUTATION** **Piece 1:** Discussions around jealousy. Scenarios around feeling jealous of things that people have posted on social media	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
		Piece 4: Discussions around what it means to be an internet troll and around stopping and thinking before sending anything on the internet or on phones, especially when reacting to something that has made them upset/angry. **COPYRIGHT AND OWNERSHIP** -I can explain why copying someone else's work from the internet without permission can cause problems (Y3) -I can give examples of what those problems might be (Y3) -When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it (Y4) -I can give some simple examples (Y4)	that there are more important things. **Piece 3:** Children to think about how to make new goals from those scenarios and think about advice they would give someone. **Computing** **SELF-IMAGE AND IDENTITY** -I can describe ways in which people might make themselves look different online. **COPYRIGHT AND OWNERSHIP** -When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it.	**Piece 6:** Discussions around what is right or wrong. Scenarios about someone sending untrue messages on social media. Children to think about how they can be more assertive in the situations (not following other people, and standing up for themselves and not doing it)	and around people posting fake images. **Piece 4:** Discussions around posting things on social media that might affect friendships.	
Year 5	**Computing** **COPYRIGHT AND OWNERSHIP** -I can assess and justify when it is acceptable to use the work of others	**Celebrating Difference** **ONLINE BULLYING** **Piece 3:** Discussions around bullying – rumours and name calling, linking to cyber-bullying. **Piece 4:** Discussions around types of bullying		**Healthy Me** **HEALTH WELLBEING AND LIFESTYLE** **Piece 4:** Discussions around body image. Discussions around how this can be affected through altered images on social media.	**Relationships** **ONLINE RELATIONSHIPS** **Pieces 2-6:** (Online safety lessons) In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
	-I can give examples of content that is permitted to be reused	including direct and indirect. Links to Cyber bullying. **Computing** **COPYRIGHT AND OWNERSHIP** **PRIVACY AND SECURITY** -I can explain why copying someone else's work from the internet without permission can cause problems.			others. Rights and responsibilities about being online, staying safe, and relationships with technology all make reference to online image and identity within these lessons. **ONLINE REPUTATION** **Pieces 2-6:** (General online safety lessons) In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to others. Rights and responsibilities about being online, staying safe, relationships with technology and online communities and gaming are discussed and learnt about in detail. **ONLINE BULLYING** **Piece 2:** Being in an online Community This lesson covers the rights and responsibilities of being online, and how an online community can help or hinder an individual.	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
					MANAGING ONLINE INFORMATION **Pieces 2-6:** (General online safety lessons) In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to others. Rights and responsibilities about being online, staying safe, relationships with technology and online communities and gaming are discussed and learnt about in detail. **HEALTH WELLBEING AND LIFESTYLE** PRIVACY AND SECURITY **Pieces 2-6:** (General online safety lessons) In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to others. Rights and responsibilities about being online, staying safe, relationships with technology and online communities and gaming are discussed and learnt about in detail. Screen time is a focus of Piece 5, as children learn to recognise	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
					when they are spending too long on their devices – and to know how to help themselves **Piece 6:** Relationships and technology Under the banner of keeping safe online, children learn about resisting pressure to use technology that could be risky or may cause harm to themselves or others. **COPYRIGHT AND OWNERSHIP** General online safety lessons) In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to others. Rights and responsibilities about being online, staying safe, relationships with technology and online communities and gaming are discussed and learnt about in detail. Piece 4 focuses on the gaming community, where children can learn about some legalities of the internet, including what age limits and use limits exist within some online communities.	

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Year 6	**Computing** **MANAGING ONLINE INFORMATION** -I can describe and assess the benefits and the potential risks of sharing information online. -I can use various additional tools to refine my searches (e.g. search filters: size, type, usage rights etc.). -I can explain how to use search effectively and use examples from my own practice to illustrate this. -I can explain how search engine rankings are returned and can explain how they can be influenced (e.g. commerce, sponsored results).	**Celebrating Difference** **ONLINE BULLYING** **Piece 4:** Why bully? Children are encouraged to practice and use a variety of strategies in managing their feelings in bullying scenarios – and how they can help solve problems if they are part of a bullying situation.	**Computing** **ONLINE RELATIONSHIPS** I can use the internet with adult support to communicate with people I know. (EY-7) **MANAGING ONLINE INFORMATION** I can navigate online content, websites, or social media feeds using more sophisticated tools to get to the information I want (e.g. menus, sitemaps, breadcrumb-trails, site search functions). (11-14) **COPYRIGHT AND OWNERSHIP** -I can explain why copying someone else's work from the internet without permission can cause problems. -I can give examples of what those problems might be. -When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it.	**Healthy Me** **HEALTH WELLBEING AND LIFESTYLE** **Piece 1:** Discussions around taking responsibility for well-being. Agony Aunt scenarios about being sleepy from playing video games. **Computing** **MANAGING ONLINE INFORMATION** -I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites) -I can use different search technologies -I can evaluate digital content and can explain how I make choices from search results	**Relationships** **SELF IMAGE AND IDENTITY** **Piece 1:** Children learn to have an accurate picture of who they are in terms of their characteristics and personal qualities. **Pieces 2-3:** In these lessons on staying safe when using technology, children learn to recognise and resist pressure to use technology in ways that may be risky or cause harm to others. Rights and responsibilities are being online, staying safe, and relationships with technology all make reference to online image and identity within these lessons. **ONLINE RELATIONSHIPS** **Pieces 5 & 6:** (Online safety lessons) Children learn to use technology positively and safely to communicate with friends and family, whilst taking	**Changing Me** **HEALTH WELLBEING AND LIFESTYLE** **Piece 1:** Discussions around body and self-image. Can introduce discussions that link to social media influences on self/body image. **ONLINE REPUTATION** **Piece 2:** Discussions around boyfriends/girlfriends. Discussions around sexting. **ONLINE RELATIONSHIPS** **HEALTH WELLBEING AND LIFESTYLE** **Piece 4:** Discussions around making choices based on peer pressure, such as playing games that are

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
			-I can give some simple examples. -I can assess and justify when it is acceptable to use the work of others. -I can give examples of content that is permitted to be reused. -I can demonstrate the use of search tools to find and access online content which can be reused by others. -I can demonstrate how to make references to and acknowledge sources I have used from the internet. -I can explain the principles of fair use and apply this to case studies. (11-14)		responsibility for their own safety and well-being. Piece 6 focuses on the SMARRT rules and how to stay safe and happy online – and what to do if you don't feel safe. **ONLINE REPUTATION** **Piece 6:** Using technology Responsibly This lesson offers the opportunity for children to learn to use technology positively and safely, so they can communicate respectfully. **MANAGING ONLINE INFORMATION** **SELF-IMAGE AND IDENTITY** **Piece 5:** Being online: real or fake? Safe or unsafe? This lesson helps children determine whether that they see online is safe and helpful – and whether it is true or fake. It also helps them to learn about resisting pressure online and becoming more discerning. The Jigsaw SMARRT rules are	not age appropriate, even though friends are. **HEALTH WELLBEING AND LIFESTYLE** **Piece 5:** Discussions around real/ideal self and influences from social media.

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
					followed in this lesson, meaning that children have agency over their actions and know where to go for help if they need it.	