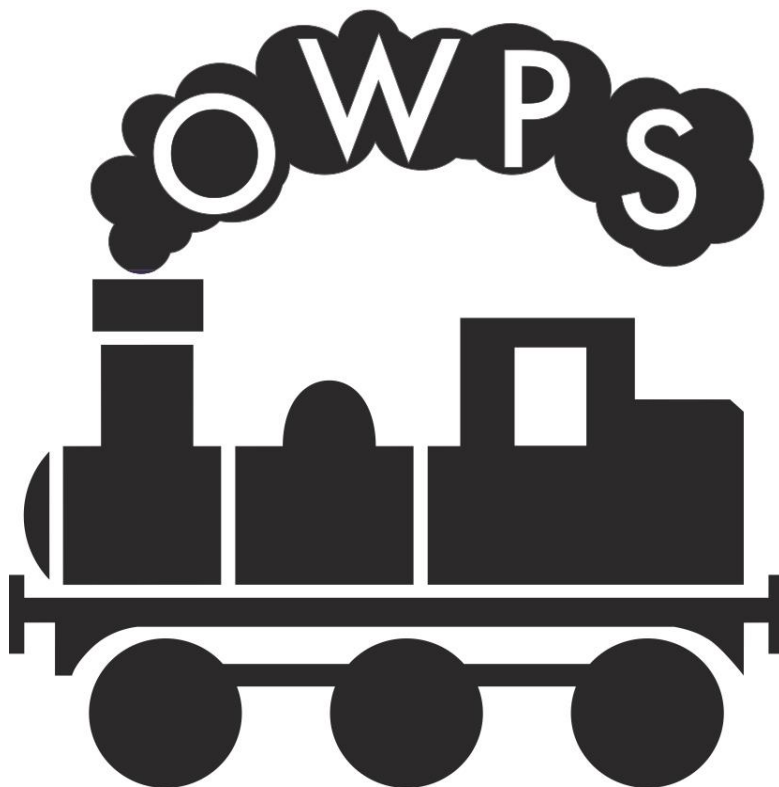


Orton Wistow Primary School



Online Safety Policy

Status	Non-Statutory Guidance
Senior Lead	Headteacher
Version	FINAL

Approved by: LGB

Date: 12/2023

Last reviewed on: Autumn 2023

Next review due by: Autumn 2025

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and *students* learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school

The implementation of this online safety policy will be monitored by the:	<i>Headteacher</i>
Monitoring will take place at regular intervals:	<i>See policy timetable</i>
The Governing Body / Governors Sub Committee will receive a report on the implementation of the online safety policy (which will include anonymous details of online safety incidents) at regular intervals:	<i>Headteachers report</i>
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>Autumn 2025</i>

Responsibilities

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Governors Sub Committee* receiving regular information about online safety incidents and monitoring reports

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community

The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
 - Inform parents of any online safety issues that the school has become aware of.

Network Manager / Technical staff:

ICT Technician must ensure

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the Local Authority Online safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online safety Co-ordinator
- digital communications with students / pupils should be on a professional level

Designated person for child protection / Child Protection Officer

should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, information about national / local online safety campaigns / literature, Information evenings at school, Parent workshops hosted at school* Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Attending events held at the school aimed to support them in keeping their children safe
- Informing the school of any potential or existing online safety issues they are aware of.

Education–students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities (online safety co-ordinator responsibility)
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- A group of students from across KS2 will make up an Online Safety team (Wistow Online Safety Rangers) that will deliver and facilitate some online safety awareness sessions within their classes or alongside the Online Safety lead in assemblies.
- Students will access and participate in school council meetings/class circle time, whole school and key stage assemblies delivered by teaching staff throughout the year which highlight and respond to current Online safety practice and curriculum focus.

Education–parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- *Information evenings*
- *Letters, newsletters, web site,*
- *Reference to the appropriate websites containing information about Online safety*

Education & Training–Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online safety lead (or other nominated person) will receive regular updates from attending events and from online safety coordinator forums
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety lead will provide advice / guidance / training as required to individuals as required

Training–Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:

- Participation in school training / information sessions for staff or parents

Technical–infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other group).

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- A scheme of work will be in place, covering topics suitable for the children within each team across the school. This will include clear links with the anti-bullying policy, covering the following topic: Electronic / 'cyberbullying' – via text message; via instant messenger services and social network sites; via email; and via images or videos posted on the internet or spread via mobile phones.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, used on the school's Facebook and Twitter feeds or used by local media (may be covered as part of the AUP signed by parents or carers at the start of the year)
- Student's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones or other camera devices				X				X
Use of hand held devices eg PDAs, PSPs	X					X		
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of chat rooms / facilities		X						X
Use of instant messaging		X						X

Use of social networking sites		X						X
Use of blogs	X					X		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				X	
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social networking sites		x			
Use of video broadcasting eg Youtube		x			

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The following will happen:

If inappropriate or illegal material is found:

- The computer will be disconnected
- If illegal the police will be contacted
- If inappropriate the LA will be contacted

If inappropriate or illegal material is suspected to have been accessed:

- Log files can be obtained if times are known
- If they are not involved discuss the details with the ICT technician
- If log files contain illegal material contact police
- If log files contain inappropriate material contact LA

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X			X	X		X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X				X		X	
Unauthorised use of social networking / instant messaging / personal email	X	X			X	X		X	
Unauthorised downloading or uploading of files	X	X			X	X		X	
Allowing others to access school network by sharing username and passwords	X							X	
Attempting to access or accessing the school network, using another student's / pupil's account	X							X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X				X		X	
Corrupting or destroying the data of other users	X	X				X		X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X		X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X		X	

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X				X	X		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X		X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X	X	X
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X		X	X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

OWPS Online Safety Curriculum:

EYFS	
AUTUMN	Media Balance is important (media balance and wellbeing) <ul style="list-style-type: none"> • Know when and why to take breaks from device time. • Consider the feelings of people around them, even when engaged in fun online activities.
SPRING	Pause for People (media balance and wellbeing) <ul style="list-style-type: none"> • Learn why it's important to be aware and respectful of people while using devices. • Learn the Pause, Breathe, Finish Up routine as a self-regulation strategy for transitioning from technology to face-to-face interactions.
SUMMER	Safety in my online neighbourhood (privacy & security) <ul style="list-style-type: none"> • Discover that the internet can be used to visit faraway places and learn new things. • Compare how staying safe online is similar to staying safe in the real world. • Explain rules for traveling safely on the internet.

Year 1	
AUTUMN	Pause and Think Online <ul style="list-style-type: none"> • Understand the importance of being safe, responsible, and respectful online. • Learn the "Pause & Think Online" song to remember basic digital citizenship concepts.
SPRING	How Technology Makes You Feel (media balance & well-being) <ul style="list-style-type: none"> • Recognize the different kinds of feelings they can have when using technology. • Know what to do when they don't have a good feeling when using technology.
SUMMER	Internet Traffic Light (privacy & security) <ul style="list-style-type: none"> • Understand that being safe online is similar to staying safe in real life. • Learn to identify websites and apps that are "just right" and "not right" for them. • Know how to get help from an adult if they are unsure about a website.

Year 2	
AUTUMN	Device Free Moments (media and well-being) <ul style="list-style-type: none"> • Recognize the ways in which digital devices can be distracting. • Identify how they feel when others are distracted by their devices. • Identify ideal device-free moments for themselves and others. That's Private (privacy and security) <ul style="list-style-type: none"> • Recognize the kind of information that is private. • Understand that they should never give out private information online.
SPRING	Digital Trails (digital footprint and identity) <ul style="list-style-type: none"> • Learn that the information they share online leaves a digital footprint or "trail" • Explore what information is OK to be shared online Who is in your online community? (relationships and communication) <ul style="list-style-type: none"> • Compare and contrast how they are connected to different people and places, in person and on the internet • Demonstrate an understanding of how people can connect on the internet
SUMMER	Putting a STOP to online meanness (We are kind & courageous) <ul style="list-style-type: none"> • Understand what online meanness can look like and how it can make people feel • Identify ways to respond to mean words online, using S-T-O-P Let's Give Credit (we are critical thinkers and creators) <ul style="list-style-type: none"> • Explain how giving credit is a sign of respect for people's work • Learn how to give credit in their schoolwork for content they use from the internet

Year 3

AUTUMN	<p>Your Rings of Responsibility (media balance and well-being)</p> <ul style="list-style-type: none"> •Examine both in-person and online responsibilities. •Describe the Rings of Responsibility as a way to think about how our behavior affects ourselves and others. •Identify examples of online responsibilities to others. <p>Password Power-Up (privacy and security)</p> <ul style="list-style-type: none"> •Define the term "password" and describe a password's purpose. •Understand why a strong password is important. •Practice creating a memorable and strong password.
SPRING	<p>This Is Me (digital footprint and identity)</p> <ul style="list-style-type: none"> •Consider how posting selfies or other images will lead others to make assumptions about them. •Reflect on the most important parts of their unique identity. •Identify ways they can post online to best reflect who they are. <p>Our Digital Citizenship Pledge (relationships & communication)</p> <ul style="list-style-type: none"> •Define what a community is, both in person and online. •Explain how having norms helps people in a community achieve their goals. •Create and pledge to adhere to shared norms for being in an online community.
SUMMER	<p>The Power of Words (we are kind & courageous)</p> <ul style="list-style-type: none"> •Understand that it's important to think about the words we use, because everyone interprets things differently. •Identify ways to respond to mean words online, using S-T-O-P. •Decide what kinds of statements are OK to say online and which are not. <p>Is Seeing Believing? (we are critical thinkers and creators)</p> <ul style="list-style-type: none"> •Recognize that photos and videos can be altered digitally. •Identify different reasons why someone might alter a photo or video. •Analyze altered photos and videos to try to determine why.

Year 4	
AUTUMN	<p>My Media Choices (media balance and well-being)</p> <ul style="list-style-type: none"> •Learn the "What? When? How Much?" framework for describing their media choices. •Use this framework and their emotional responses to evaluate how healthy different types of media choices are. •Begin to develop their own definition of a healthy media balance. <p>Private and Personal Information (privacy and security)</p> <ul style="list-style-type: none"> •Identify the reasons why people share information about themselves online. •Explain the difference between private and personal information. •Explain why it is risky to share private information online.
SPRING	<p>Our Online Tracks (digital footprint and identity)</p> <ul style="list-style-type: none"> •Define the term "digital footprint" and identify the online activities that contribute to it. •Identify ways they are -- and are not -- in control of their digital footprint. •Understand what responsibilities they have for the digital footprints of themselves and others. <p>Keeping Games Fun & Friendly (relationships & communication)</p> <ul style="list-style-type: none"> •Define "social interaction" and give an example. •Describe the positives and negatives of social interaction in online games. •Create an online video game cover that includes guidelines for positive social interaction.
SUMMER	<p>Be a Super Digital Citizen (we are kind & courageous)</p> <ul style="list-style-type: none"> •Reflect on the characteristics that make someone an upstanding digital citizen. •Recognize what cyberbullying is. •Show ways to be an upstander by creating a digital citizenship superhero comic strip. <p>A Creator's Rights and Responsibilities (we are critical thinkers and creators)</p> <ul style="list-style-type: none"> •Define "copyright" and explain how it applies to creative work.

	<ul style="list-style-type: none"> •Describe their rights and responsibilities as creators. •Apply copyright principles to real-life scenarios.
--	---

Year 5	
AUTUMN	<p>Finding My Media Balance (media balance and well-being)</p> <ul style="list-style-type: none"> •Reflect on how balanced they are in their daily lives. •Consider what "media balance" means, and how it applies to them. •Create a personalized plan for healthy and balanced media use. <p>You Won't Believe This (privacy and security)</p> <ul style="list-style-type: none"> •Define "the curiosity gap." •Explain how clickbait uses the curiosity gap to get your attention. •Use strategies for avoiding clickbait.
SPRING	<p>Beyond Gender Stereotypes (digital footprint & identity)</p> <ul style="list-style-type: none"> •Define "gender stereotype" and describe how they can be present online. •Describe how gender stereotypes can lead to unfairness or bias. •Create an avatar and a poem that show how gender stereotypes impact who they are. <p>You Won't Believe This (privacy and security)</p> <ul style="list-style-type: none"> •Define "the curiosity gap." •Explain how clickbait uses the curiosity gap to get your attention. •Use strategies for avoiding clickbait.
SUMMER	<p>Is It Cyberbullying? (we are kind & courageous)</p> <ul style="list-style-type: none"> •Recognize similarities and differences between in-person bullying, cyberbullying, and being mean. •Empathize with the targets of cyberbullying. •Identify strategies for dealing with cyberbullying and ways they can be an upstander for those being bullied. <p>You Won't Believe This (privacy and security)</p> <ul style="list-style-type: none"> •Define "the curiosity gap." •Explain how clickbait uses the curiosity gap to get your attention. •Use strategies for avoiding clickbait.

Year 6	
AUTUMN	<p>Finding Balance in a Digital World (media balance and well-being)</p> <ul style="list-style-type: none"> •Reflect on their common online and offline activities. •Identify ways to "unplug" to maintain balance between online and offline activities. •Use the Digital Habits Checkup routine to create a personal challenge to achieve more media balance. <p>Don't Feed The Phish (privacy and security)</p> <ul style="list-style-type: none"> •Compare and contrast identity theft with other kinds of theft. •Describe different ways that identity theft can occur online. •Use message clues to identify examples of phishing.
SPRING	<p>Who are you online? (digital footprint & identity)</p> <ul style="list-style-type: none"> •Reflect on reasons why people might create fake social media accounts. •Identify the possible results of posting from a fake social media account. •Debate the benefits and drawbacks of posting from multiple accounts. <p>Chatting safely online (relationships & communication)</p> <ul style="list-style-type: none"> •Analyze how well they know the people they interact with online. •Reflect on what information is safe to share with different types of online friends. •Learn to recognize red flag feelings and use the Feelings & Options thinking routine to respond to them.
SUMMER	<p>Digital Drama Unplugged (we are kind and courageous)</p> <ul style="list-style-type: none"> •Reflect on how easily drama can escalate online. •Identify de-escalation strategies when dealing with digital drama.

- | | |
|--|--|
| | <ul style="list-style-type: none">• Reflect on how digital drama can affect not only oneself but also those around us. <p>Finding Credible News (We are critical thinkers & creators)</p> <ul style="list-style-type: none">• Learn reasons that people put false or misleading information on the internet.• Learn criteria for differentiating fake news from credible news.• Practice evaluating the credibility of information they find on the internet. |
|--|--|