Digital Safety Policy

June 2026

Next Review: June 2027

Approved by: Headteacher

Computing Lead:	**Miss J Roome**
Lead DSL for Filtering and Monitoring:	**Mrs Niki Lineker**
Lead Governor for Filtering and Monitoring:	**Mr Rupert Boddington**

Introduction

The Internet and other digital and information technologies are greatly beneficial tools to children's learning but children need to be aware of how to use these tools appropriately and safely. This digital safety policy highlights how Glade Hill Primary and Nursery believes that every child should have the right to a curriculum that champions excellence; supporting pupils in achieving to the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

This policy should be read in conjunction with other relevant school policies such as Safeguarding & Child Protection, Use of AI, Equality, Curriculum, SEND and Assessment policies. The policy has been developed by the Computing Leader (Miss Roome) in consultation with the Lead DSL for Filtering and Monitoring (Niki Lineker), SENCO, Leadership Team and teachers. Guidance from consultants and pupil, parent and staff voice questionnaires have shaped and will continue to help shape this policy. This policy is based on government recommended/statutory programmes of study, particularly those from the Filtering and Monitoring Standards for Schools and Colleges guidance (DFE updated 2026). Due to the fast pace of technology innovation and constantly emerging trends, it is recommended that this policy is reviewed, at minimum, at the start of every academic cycle or more regularly in light of any significant new developments in the use of new technologies, new threats to digital safety or incidents that have taken place.

1 Roles and Responsibilities

Digital safety is an integral part of the safeguarding duties we have to our pupils at Glade Hill Primary School; we place a high importance on all staff and governors taking responsibility for educating and modelling to pupils the safe use of all devices both within and outside of school. As Digital Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. We acknowledge the importance of our pupils taking responsibilities for safe use, and having the opportunity to contribute to relevant policies.

We have assigned the following key roles to ensure the delivery and maintenance of effective filtering and monitoring systems:

Designated Safeguarding Governor:
Mr Rupert Boddington

Lead DSL for Filtering and Monitoring:
Mrs Niki Lineker

Computing Lead:
Miss Jaimieleigh Roome

Outlined below are the roles and responsibilities for all:

Governors:

- Ensuring school has relevant and up to date policies in place regarding Digital Safety and a Lead DSL for Filtering and Monitoring
- Review policies annually and in response to any Digital Safety concern/ incident review the effectiveness of the policy when managing such incidents with the Headteacher, DSL and Computing Lead.
- Undertake basic cyber security awareness training and support school cyber security oversight.
- To support the school in encouraging parents and the wider community to become engaged in online safety activities.

Designated Safeguarding Governor:

- Liaise with DSL and Computing Lead to understand the role Digital Safety plays in safeguarding within school, its role within the curriculum, how it is taught and planned for.
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with DfE standards.
- Ensure Digital Safety is on the agenda and discussed at regular governors meetings.

Headteacher:

- Overall responsibility for Digital Safety as a safeguarding issue, ensuring that policies and procedures are embedded, although day to day running will be delegated to the Computing Leader and DSL.
- Ensure opportunities for Digital Safety training throughout the school are planned for, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents.
- Ensure there is at least one DSL in school who has appropriate training to report and manage E safety incidents.
- Ensuring all E-Safety incidents are dealt with promptly and appropriately in line with school policy.
- To be aware of procedures to be followed in the event of a serious online safety incident.
- Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised.
- To ensure the school website includes the relevant information.

Lead DSL for Filtering and Monitoring:

- Be the first point of contact for anyone reporting an E-Safety safeguarding issues, ensuring the incident is logged on the correct form: Online Safety Incident Form (see Appendix 1) and dealt with according to school policy.
- To liaise with and inform the Headteacher, other DSLs and Computing Lead of any E-Safety incidents and provide Lead Governor with termly incident reports and updates where necessary.

- Ensure Digital Safety concerns/incidents are on the agenda for fortnightly safeguarding meetings with DSLs.
- Liaise closely with the Computing Lead regarding record keeping and logging of E-Safety incidents or ineffective filtering.
- Liaise with the Local Authority and relevant agencies.
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Ensures they are regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.

Computing Lead:

- Ensure that online safety is embedded within the curriculum.
- Liaise with Designated Safeguarding Governor to monitor effectiveness of the Digital Safety policy and implementation of the Digital Safety curriculum across school.
- Monitor the effectiveness and impact of the Digital Safety policy and curriculum across school, reporting back to staff and governors.
- Keep up to date with the latest risks to children whilst using technology; familiarising themselves with the latest research and available resources for school and home use.
- Ensure an up to date Digital Safety policy, which is reflective of current legislation and best practice, reviewing in response to any E-Safety incidents bringing any concerns to the attention of the Headteacher and Lead DSL.
- Advise the Headteacher, Governors and staff on Digital Safety matters and best practise through INSET and staff meeting training, ensuring staff have full awareness of current guidelines and requirements.
- Engage with parents and school community regarding Digital Safety matters, develop a parental awareness programme including updating regularly the Digital Safety pages of the website with the most current advice and work from the children.
- Liaise with the local authority, IT technical support and other agencies as required e.g. ensuring any technical E-Safety measures in school (e.g. Internet filtering software) are fit for purpose.
- Liaise with Lead DSL and share responsibility for the Digital Safety incident log and iPad usage logs and ensure staff know what to report, how and where.

SCHOOLS IT technical support:

- Provide a technical infrastructure to support Digital Safety practices.
- Ensure the IT technical infrastructure is secure and the network and server are secure.
- Ensure the anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Ensure Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Ensure any Digital Safety technical solutions such as Internet filtering are operating correctly.

- Ensure filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Lead DSL and Computing Lead.
- Passwords for staff will be a minimum of 8 characters (and will be alphanumeric).
- Two factor authentication is set up on all staff emails.
- The IT System Administrator password is to be changed on a monthly (30 day) basis and is only kept by IT support not staff members.
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Headteacher.
- They will also work with the senior leadership team and Lead DSL to procure systems, identify risk, carry out reviews and carry out regular checks.
- Provide the Lead DSL with timely filtering reports.

All teachers and support staff:

Safeguarding pupils when using devices is the responsibility of all. They will:

- Ensure the safe use of devices by all pupils and ensure pupils are supervised at all times.
- Deal with Digital Safety issues as soon as they become aware of them and know how to report concern or incidents to the Lead DSL.
- Ensure they follow all policies including the Digital Safety Policy, acting as a model of safe and responsible use of technologies and the internet to pupils.
- Adhere to acceptable use policies and the Staff Code of Conduct, with particular regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- Take responsibility for the security of data.
- Develop an awareness of Digital Safety issues and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Teach Digital Safety regularly as part of the Computing, PSHE and Glade Hill Curriculum.
- Follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- All digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices
- Where staff use AI, they should only use school-approved AI services for work purposes and verify / fact check outputs for accuracy/bias before use.
- Be aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. Staff should disclose AI usage in external communications/publications e.g. “This email/document contains content generated by AI. It has been reviewed for accuracy.”
- AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

See Appendix 2 for Safe Use of Devices children and staff posters which are to be displayed in every classroom and learning space.

2 Teaching and Learning

2.1 Why the internet is important

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Information will be provided to parents about how to educate and support their children with safe internet use- see parents guides.

2.2 Internet use will enhance learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school recognises it has a duty to provide pupils with high-quality internet access as part of their learning experience in school and prepare them to make safe and effective use out of school.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to become responsible, respectful and competent users of data, information and communication technology.
- Pupils will be equipped with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise the risk to themselves or others.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with the copyright law.
- Pupils will be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information.

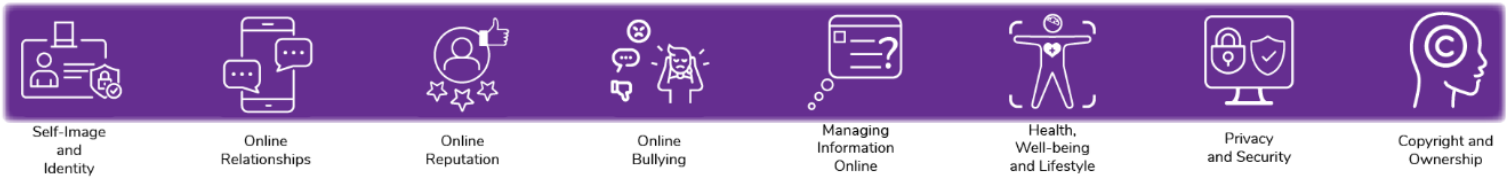
- Pupils should compare web material with other sources and be able to evaluate which is more useful. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.
- Pupils will be taught how to think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content.
- All pupils will be taught that if they access any information or images which they think are inappropriate or make them uncomfortable, they should close the page and report the incident immediately to the teacher who will pass the report onto the Lead DSL for Filtering and Monitoring and the Headteacher.

2.4 Digital Safety Curriculum

Please find below a copy of our Digital Safety programme of study within our Computing curriculum. This is taught through a sequential and progressive programme of work using the Purple Mash 2BeSafe: Being Safe in a Digital World scheme of learning.

2BeSafe is an online safety scheme of work, published by 2Simple, to meet the guidance set out within the Department for Education's - Education for a Connected World. The Education for a Connected World framework outlines eight key areas which seek to equip children and young people for digital life and the digital world. 2Simple's 2BeSafe offers a comprehensive coverage of these requirements for primary schools starting from Reception up to Year 6.

Units covered:



As well as this, Digital Safety is also integral to our PSHE Curriculum and this is taught though different themes throughout the year. Cyber bullying is a strong element of discussion on annual anti-bullying weeks as well as whole school assemblies throughout the year.

Below are the objectives covered in the 2BeSafe scheme of work:

EYFS:

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online	Copyright and Ownership
Lesson 1	I can recognise, online or offline, that anyone can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who makes them feel sad, uncomfortable, embarrassed or upset.	I can recognise some ways in which the internet can be used to communicate.	I can identify ways that I can put information on the internet.	I can describe ways that some people can be unkind online.	I can identify rules that help keep us safe and healthy in and beyond the home when using technology. I can give some simple examples of these rules.	I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location).	I can talk about how to use the internet as a way of finding information online.	I know that work I create belongs to me.
Lesson 2		I can give examples of how I (might) use technology to communicate with people I know.		I can offer examples of how this can make others feel.		I can describe who would be trustworthy to share this information with; I can explain why they are trusted.	I can identify devices I could use to access information on the internet.	I can name my work so that others know it belongs to me.

Year 1

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online Information	Copyright and Ownership
Lesson 1	I can recognise that there may be people online who could make someone feel sad, embarrassed or upset.	I can give examples of when I should ask permission to do something online and explain why this is important.	I can recognise that information can stay online and could be copied.	I can describe how to behave online in ways that do not upset others and can give examples.	I can explain rules to keep myself safe when using technology both in and beyond the home.	I can explain that passwords are used to protect information, accounts and devices.	I can give simple examples of how to find information using digital technologies, e.g. search engines, voice activated searching).	I can explain why work I create using technology belongs to me.
Lesson 2	If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.	I can use the internet with adult support to communicate with people I know (e.g. video call apps or services).	I can describe what information I should not put online without asking a trusted adult first.			I can recognise more detailed examples of information that is personal to someone (e.g where someone lives and goes to school, family names).	I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke.	I can say why it belongs to me (e.g. 'I designed it' or 'I filmed it').
Lesson 3		I can explain why it is important to be considerate and kind to people online and to respect their choices.				I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others.	I know how to get help from a trusted adult if we see content that makes us feel sad, uncomfortable worried or frightened.	I can save my work under a suitable title / name so that others know it belongs to me (e.g. filename, name on content).
Lesson 4		I can explain why things one person finds funny or sad online may not always be seen in the same way by others.						I understand that work created by others does not belong to me even if I save a copy.

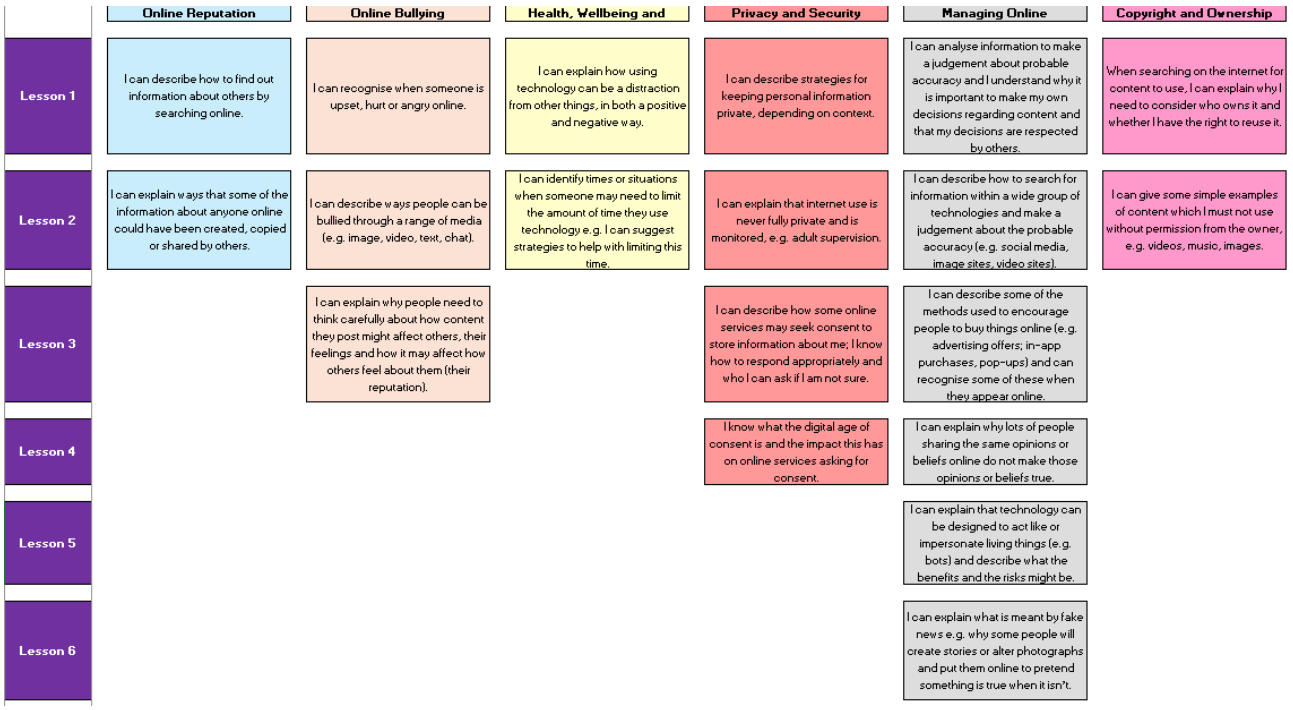
Year 2

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online	Copyright and Ownership
Lesson 1	I can explain how other people may look and act differently online and offline.	I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country).	I can explain how information put online about someone can last for a long time.	I can explain what bullying is, how people may bully others and how bullying can make someone feel.	I can explain simple guidance for using technology in different environments and settings e.g. accessing online technologies in public places and the home environment. I can say how those rules / guides can help anyone accessing online technologies.	I can explain how passwords can be used to protect information, accounts and devices.	I can use simple keywords in search engines.	I can recognise that content on the internet may belong to other people
Lesson 2	I can give examples of issues online that might make someone feel sad, worried, uncomfortable or frightened; I can give examples of how they might get help.	I can explain who I should ask before sharing things about myself or others online.	I can describe how anyone's online information could be seen by others.	I can explain why anyone who experiences bullying is not to blame.		I can explain and give examples of what is meant by 'private' and 'keeping things private'.	I can demonstrate how to navigate a simple webpage to get to information I need (e.g. home, forward, back buttons; links, tabs and sections).	I can describe why other people's work belongs to them.
Lesson 3		I can describe different ways to ask for, give, or deny my permission online and can identify who can help me if I am not sure.	I know who to talk to if something has been put online without consent or if it is incorrect.	I can talk about how anyone experiencing bullying can get help.		I can describe and explain some rules for keeping personal information private (e.g. creating and protecting passwords).	I can explain what voice activated searching is and how it might be used, and know it is not a real person (e.g. Alexa, Google Nov, Siri).	
Lesson 4		I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do.				I can explain how some people may have devices in their homes connected to the internet and give examples (e.g. lights, fridges, toys, televisions).	I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'.	
Lesson 5		I can identify who can help me if something happens online without my consent.					I can explain why some information I find online may not be real or true.	
Lesson 6		I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them online.						
Lesson 7		I can explain why I should always ask a trusted adult before clicking 'yes', 'agree' or 'accept' online.						

Year 3

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online	Copyright and Ownership
Lesson 1	I can explain what is meant by the term 'identity'.	I can describe ways people who have similar likes and interests can get together online.	I can explain how to search for information about others online.	I can describe appropriate ways to behave towards other people online and why this is important.	I can explain why spending too much time using technology can sometimes have a negative impact on anyone, e.g. mood, sleep, body, relationships; I can give some examples of both positive and negative activities where it is easy to spend a lot of time engaged (e.g. doing homework, games, films, videos).	I can describe simple strategies for creating and keeping passwords private.	I can demonstrate how to use key phrases in search engines to gather accurate information online.	I can explain why copying someone else's work from the internet without permission isn't fair and can explain what problems this might cause.
Lesson 2	I can explain how people can represent themselves in different ways online.	I can explain what it means to "know someone" online and why this might be different from knowing someone offline.	I can give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal.	I can give examples of how bullying behaviour could appear online and how someone can get support.	I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable (e.g. age restricted gaming or web sites).	I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure or feel pressured then they should tell a trusted adult.	I can explain what autocomplete is and how to choose the best suggestion.	
Lesson 3	I can explain ways in which someone might change their identity depending on what they are doing online (e.g. gaming; using an avatar; social media) and why.	I can explain what is meant by "trusting someone online", why this is different from "liking someone online", and why it is important to be careful about who to trust online including what information and content they are trusted with.	I can explain who someone can ask if they are unsure about putting something online.			I can describe how connected devices can collect and share anyone's information with others.	I can explain how the internet can be used to sell and buy things.	
Lesson 4		I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried.					I can explain the difference between a "belief", an "opinion" and a "fact, and can give examples of how and where they might be shared online, e.g. in videos, memes, posts, news stories etc.	
Lesson 5		I can explain how someone's feelings can be hurt by what is said or written online.					I can explain that not all opinions shared may be accepted as true or fair by others (e.g. monsters under the bed).	
Lesson 6		I can explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline e.g. sharing images and videos.					I can describe and demonstrate how we can get help from a trusted adult if we see content that makes us feel sad, uncomfortable worried or frightened.	

Year 4



	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online	Copyright and Ownership
Lesson 1	I can describe how to find out information about others by searching online.	I can recognise when someone is upset, hurt or angry online.	I can explain how using technology can be a distraction from other things, in both a positive and negative way.	I can describe strategies for keeping personal information private, depending on context.	I can analyse information to make a judgement about probable accuracy and I understand why it is important to make my own decisions regarding content and that my decisions are respected by others.	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.
Lesson 2	I can explain ways that some of the information about anyone online could have been created, copied or shared by others.	I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat).	I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.	I can explain that internet use is never fully private and is monitored, e.g. adult supervision.	I can describe how to search for information within a wide group of technologies and make a judgement about the probable accuracy (e.g. social media, image sites, video sites).	I can give some simple examples of content which I must not use without permission from the owner, e.g. videos, music, images.
Lesson 3		I can explain why people need to think carefully about how content they post might affect others, their feelings and how it may affect how others feel about them (their reputation).		I can describe how some online services may seek consent to store information about me; I know how to respond appropriately and who I can ask if I am not sure.	I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases, pop-ups) and can recognise some of these when they appear online.	
Lesson 4				I know what the digital age of consent is and the impact this has on online services asking for consent.	I can explain why lots of people sharing the same opinions or beliefs online do not make those opinions or beliefs true.	
Lesson 5					I can explain that technology can be designed to act like or impersonate living things (e.g. bots) and describe what the benefits and the risks might be.	
Lesson 6					I can explain what is meant by fake news e.g. why some people will create stories or alter photographs and put them online to pretend something is true when it isn't.	

Year 5

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online Information	Copyright and Ownership
Lesson 1	I can explain how identity online can be copied, modified or altered.	I can give examples of technologyspecific forms of communication (e.g. emojis, memes and GIFs).	I can search for information about an individual online and summarise the information found.	I can recognise online bullying can be different to bullying in the physical world and can describe some of those differences.	I can describe ways technology can affect health and well-being both positively (e.g. mindfulness apps) and negatively.	I can explain what a strong password is and demonstrate how to create one.	I can explain the benefits and limitations of using different types of search technologies e.g. voice-activation search engine. I can explain how some technology can limit the information I aim presented with e.g. voice-activated searching giving one result.	I can *assess* and justify when it is acceptable to use the work of others.
Lesson 2	I can demonstrate how to make responsible choices about having an online identity, depending on context	I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my *i*r our fault.	I can describe ways that information about anyone online can be used by others to make judgments about an individual and why these may be incorrect	I can describe how what one person perceives as playful joking and teasing (including 'banter') might be experienced by others as bullying.	I can describe some strategies, tips or advice to promote health and wellbeing with regards to technology.	I can explain how many free apps or services may read and share private information (e.g. friends, contacts, likes, images, videos, voice, messages, geolocation) with others.	I can explain what is meant by 'being sceptical'; I can give examples of when and why it is important to be 'sceptical'.	I can give examples of content that is permitted to be reused and know how this content can be found online.
Lesson 3		I can describe some of the ways people may be involved in online communities and describe how they might collaborate constructively with others and make positive contributions. (e.g. gaming communities or social media groups).		I can explain how anyone can get help if they are being bullied online and identify when to tell a trusted adult.	I recognise the benefits and risks of accessing information about health and well-being online and how we should balance this with talking to trusted adults and professionals.	I can explain what app permissions are and can give some examples	I can evaluate digital content and can explain how to make choices about what is trustworthy e.g. differentiating between adverts and search results.	
Lesson 4		I can explain how someone can get help if they are having problems and identify when to tell a trusted adult.		I can identify a range of ways to report concerns and access support both in school and at home about online bullying.	I can explain how and why some apps and games may request or take payment for additional content (e.g. in-app purchases, lootboxes) and explain the importance of seeking permission from a trusted adult before purchasing.		I can explain key concepts including: information, reviews, fact, opinion, belief, validity, reliability and evidence.	
Lesson 5		I can demonstrate how to support others (including those who are having difficulties) online		I can explain how to block abusive users.			I can identify ways the internet can draw us to information for different agendas; e.g. website notifications, pop-ups, targeted ads.	
Lesson 6				I can describe the helpline services which can help people experiencing bullying, and how to access them (e.g. Childline or The Mix).			I can describe ways of identifying when online content has been commercially sponsored or boosted, (e.g. by commercial companies or by vloggers, content creators, influencers).	
Lesson 7							I can explain what is meant by the term 'stereotype', how 'stereotypes' are amplified and reinforced online, and why accepting 'stereotypes' may influence how people think about others.	
Lesson 8							I can describe how fake news may affect someone's emotions and behaviour, and explain why this may be harmful.	
Lesson 9							I can explain what is meant by a 'hoax'. I can explain why someone would need to think carefully before they share.	

Year 6

	Self-Image and Identity	Online Relationships	Online Reputation	Online Bullying	Health, Wellbeing and	Privacy and Security	Managing Online	Copyright and Ownership
Lesson 1	I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online.	I can explain how sharing something online may have an impact either positively or negatively.	I can explain the ways in which anyone can develop a positive online reputation.	I can describe how to capture bullying content as evidence (e.g screen-grab, URL, profile) to share with others who can help me.	I can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose	I can describe effective ways people can manage passwords (e.g. storing them securely or saving them in the browser).	I can explain how search engines work and how results are selected and ranked.	I can demonstrate the use of search tools to find and access online content which can be reused by others.
Lesson 2	I can describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. I know and can give examples of how to get help, both on and offline.	I can describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not.	I can explain strategies anyone can use to protect their 'digital personality' and online reputation, including degrees of anonymity.	I can explain how someone would report online bullying in different contexts.	I recognise and can discuss the pressures that technology can place on someone and how / when they could manage this.	I can explain what to do if a password is shared, lost or stolen.	I can explain how to use search technologies effectively.	I can demonstrate how to make references to and acknowledge sources I have used from the internet.
Lesson 3	I can explain the importance of asking until I get the help needed.	I can describe how things shared privately online can have unintended consequences for others. e.g. screen-grabs.			I can recognise features of persuasive design and how they are used to keep users engaged (current and future use).	I can describe how and why people should keep their softw are and apps up to date, e.g. auto updates.	I can describe how some online information can be opinion and can offer examples.	
Lesson 4		I can explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and who can help if someone is worried about this.			I can assess and action different strategies to limit the impact of technology on health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise).	I can describe simple ways to increase privacy on apps and services that provide privacy settings.	I can explain how and why some people may present 'opinions' as 'facts'; why the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal.	
Lesson 5						I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. scams, phishing).	I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how someone might encounter these online (e.g. advertising and 'ad targeting' and targeting for fake news).	

3 Managing Internet Access

3.1 Information system security

- School computing systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly

3.2 Email

- E-mail is an essential means of communication for staff.
- Currently pupils do not have school email accounts. Class email accounts are used in each class.
- Pupils will be taught in school how to safely use e-mail and guidance will be provided to parents.

3.3 Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number.
- The Headteacher will take will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing Pupils images and work

- The school has sought parental consent for any images of children that are used on the school website.
- To ensure the children's safety only first names will be published on the site, particularly in association with photographs.

3.5 Social Networking and personal publishing

- The school will block/filter access to social networking sites.
- However, parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

- Pupils will be taught about personal safety when using social networking sites outside the school and advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.6 Managing the filters

- Currently, the school use filtering through Nottingham City Schools IT Service to ensure inappropriate material (e.g. CSE, Sexual and Extremist content) is denied to pupils, and school will continue to monitor and block any inappropriate sites with support from the Schools IT Service.
- Monitoring supports the rapid identification of safeguarding concerns and enables timely intervention and this is done through the use of the Smoothwall Monitor system. Timely alerts are sent to the Lead DSL for Filtering and Monitoring and Headteacher and are dealt with immediately in line with the school behaviour and safeguarding policies.
- Schools IT will maintain filtering and monitoring systems, provide timely filtering and monitoring reports and complete actions following concerns or checks to systems. They will support the Senior Leadership Team and the Lead DSL for Filtering and Monitoring to procure systems, identify risk, carry out reviews and carry out checks.
- Reviews of filtering and monitoring systems will be carried out at least annually by the SLT, Lead DSL for Filtering and Monitoring, Schools IT and the Lead Governor for Filtering and Monitoring.
- The Computing Lead and Lead DSL for Filtering and Monitoring work alongside Schools IT to agree blocked lists and they are able to deny access to any apps or webpages we deem necessary. Schools IT keep up to date with any emerging priorities in websites or apps that need blocking and block access accordingly.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Lead DSL for Filtering and Monitoring, who will take measures to ensure site is blocked in conjunction with the Schools IT Service.
- The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- Detailed logs of any ineffective filtering or misuse of devices is kept securely and updated by the Lead DSL for Filtering and Monitoring on a shared DSL folder. These reports are shared termly with the Lead Governor for Filtering and Monitoring and all DSLs are kept up-to-date on any incidences via DSL meetings, and access to this log.

3.7 Managing emerging technologies

- Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed.
- Staff will receive CPD opportunities in the use of iPads and new software to ensure effective practice.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) 2017 and the Data Protection Act 2018.

3.9 Remote Education and Homework

- In accordance with our Remote Education Strategy, we aim to provide the same curriculum remotely as we do in school wherever possible and appropriate. However, much of this will be using online platforms such as Purple Mash to record their writing, allowing for teachers to provide children with feedback.
- Staff will ensure that resources and websites are suitable for children before setting work.
- Child friendly sites which we use frequently for setting homework or remote education tasks are MyMaths, Purple Mash, Times Table Rock Stars, BBC Bitesize, White Rose Maths Hub or Oak National Academy.
- We encourage parents to be vigilant with digital safety and ensure that children are accessing appropriate sites while at home. Digital safety advice will be available on our website at all times and will be clearly visible on class pages during times of remote education.

4 Policy Decisions

4.1 Authorising Internet Access

- The Digital Safety Policy and its application and importance will be discussed and approved by all staff.
- In Foundation and Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

4.2 Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate materials. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequence of Internet access.
- The school should audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

4.3 Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school safeguarding and child protection policy and procedures.

5 Communication

5.1 Introducing the Digital Safety Policy to pupils

- All pupils will be taught about digital safety regularly and will help to design posters about safety rules. The e-safety lessons will be structured around the Purple Mash scheme of computing work. We will also use resources from ThinkUKnow to help educate pupils about digital safety.
- Pupils and parents also receive access to the Safer Schools app which is designed to empower and educate them in staying safe online.
- Digital safety rules will be displayed in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- Instruction in responsible and safe use should precede Internet access.

5.2 Staff and the Digital Safety Policy

- The Digital Safety Policy and its application and importance will be discussed and approved by all staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretions and professional conduct are essential.
- Staff understand the importance of identifying, intervening in and escalating any concerns regarding content, contact, conduct and commerce as stated in the Keeping Child Safe in Education guidance.
- Staff understand the appropriateness of use of their own personal devices such as smart phones and watches as detailed in the Staff Code of Conduct. Staff are provided with an iPad to use for taking photographs of children's work and engagement with learning.

5.3 Parental Involvement

- Internet use (including online gaming) in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.
- Parents' attention will be drawn to the school's Digital Safety Policy in newsletters, the school prospectus and on the school website.
- Parents also have access to the Safer Schools app which is designed to support and educate them in keeping their children safe online.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged and guidance on Internet use in the home will be issued.

The following sites are useful for parents to find out more about e-safety or to use with their children.

https://www.saferinternet.org.uk

https://www.ceop.police.uk/safety-centre

https://www.nspcc.org.uk/keeping-children-safe

https://parentzone.org.uk/ https://www.thinkuknow.co.uk/

Appendix 1

Online Safety Incident Reporting Log

Date	Time	Incident	Action Taken		Incident Reported By
			What?	By Whom?	

Appendix 2

Safe Use of Digital Devices

- ✓ Children **must be supervised at all times** when using a device
- ✓ Ensure children sit in a position where you can see their screens easily
- ✓ Regularly check in on each pupil to ensure they are using the device responsibly
- ✓ During reward time make sure children show you what games they are playing on and check their suitability
- ✓ Remind children regularly on what to do if they see something upsetting or inappropriate – *turn off the screen immediately and tell an adult*

How to report a concern:

- ➢ First ensure the child's safety – *secure the device and confiscate if necessary*
- ➢ Report any safeguarding concerns immediately to:
  Mrs Lineker Lead DSL for Filtering and Monitoring
  In her absence report to any other DSL and log using My Concern
- ➢ If there is an issue with the filtering (e.g. blocking educational sites you need) or the devices, then please report to:
  Miss Roome Computing Lead
- ➢ If necessary, contact parents to inform them (check first with a DSL/SLT)

If you see something upsetting online

Stop what you are doing.

Do not click on the page or reply to the message.

Close the laptop.

Put down the iPad or phone.

Do not show your friend.

Tell a grown up straight away.