



# Digital Safety Policy

**January 2025**

**Next Review: January 2026**

**Approved by: Headteacher**

**Computing Lead:**

**Lead DSL for Filtering and Monitoring:  
(covered by Mrs Anna Stapleton currently)**

**Lead Governor for Filtering and Monitoring:**

**Miss J Roome**

**Mrs Niki Lineker**

**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, 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 2024). 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 (covered by Anna Stapleton currently)

**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.
- 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.
- Monitor effectiveness of Digital Safety policies through liaising with Computing Lead and DSL.
- 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.
- 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.
- 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.

See Appendix 2 for Safe Use of Devices staff poster which is 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.
- 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 Literacy programme of study within our Computing curriculum. This is taught through a sequential and progressive programme of work using the Purple Mash – 2simple platform. Digital Literacy starts right at the foundations of learning in the Early Years. Through different themed units as part of our curriculum, the children gain a greater understanding in Technology All Around Us, Safety and Privacy and using their own personal login. From Year 1 to Year 6 Digital Literacy is developed through units focussing on information technology and digital safety.

As well as this, Digital Safety is also integral to our PSHE Curriculum and this is taught through 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.

**EYFS:**

Technology Around Us	Unit Theme	'I can'
	 <p>Technology Around Us</p>	I can talk about what technology is used at home.
		I can talk about what technology is used outdoors.
		I can talk about what technology is used in the world around me.
Safety and Privacy	Unit Theme	'I can'
	 <p>Safety and Privacy</p>	I can explain how my work on the computer belongs to me and other people's work belongs to them.
		I can explain what it means for something to be private.
		I can talk about how my body feels when I am not comfortable with something.
		I know who can help me when I am feeling worried.
		I can show that I understand how to be kind to others.
		I can choose activities in my free time that help me to be healthy.
Using Purple Mash with an Individual Login	Unit Theme	'I can'
	 <p>Using Purple Mash with an Individual Login</p>	I can get to the Purple Mash page on my device at school and at home.
		I can login to Purple Mash \ Mini Mash in school using the shortcut icon.
		I can login to Purple Mash and Mini Mash using my username and password.
		I can login to Purple Mash a Mini Mash using my username and password.
		I can login to Purple Mash a Mini Mash using my username and password.
		I can save work in my own tray\ folder when I am using Mini\Purple Mash.
		I can open work that I have done earlier.
		I can find and complete 2Dos that my teacher has set for me

Year 1

		Information Technology	Digital Literacy	
Statement		Use technology purposefully to create, organise, store, manipulate and retrieve digital content.	Recognise common uses of information technology beyond school.	Use technology safely and respectfully, keep personal information private; identify where to go for help\ support with concerns about content or contact on the internet or other online technologies.
Outcome		Children can sort, collate, edit and store simple digital content e.g. children can name, save and retrieve their work and follow simple instructions to access online resources, use Purple Mash 2Quiz example (sorting shapes), 2Code design mode (manipulating backgrounds) or using pictogram software such as 2Count.	Children understand what is meant by technology and can identify a variety of examples both in and out of school. They can make a distinction between objects that use modern technology and those that do not e.g. a microwave vs. a chair.	Children understand the importance of keeping information, such as their usernames and passwords, private and actively demonstrate this in lessons. Children take ownership of their work and save this in their own private space such as their My Work folder on Purple Mash.

Year 2

	Information Technology	Digital Literacy	
Statement	Use technology purposefully to create, organise, store, manipulate and retrieve digital content.	Recognise common uses of information technology beyond school.	Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
Outcome	Children demonstrate an ability to organise data using, for example, a database such as 2Investigate and can retrieve specific data for conducting simple searches. Children can edit more complex digital data such as music compositions within 2Sequence. Children are confident when creating, naming, saving and retrieving content. Children use a range of media in their digital content including photos, text and sound.	Children can effectively retrieve relevant, purposeful digital content using a search engine. They can apply their learning of effective searching beyond the classroom. They can share this knowledge, e.g. 2Publish example template. Children make links between the technology they see around them, coding and multimedia work they do in school e.g. animations, interactive code and programs.	Children know the implications of inappropriate online searches. Children begin to understand how things are shared electronically such as posting work to the Purple Mash display board. They develop an understanding of using email safely by using 2Respond activities on Purple Mash and know ways of reporting inappropriate behaviours and content

Year 3

	Information Technology		Digital Literacy
Statement	Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.	Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.	Use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concern about content and contact.
Outcome	Children can carry out simple searches to retrieve digital content. They understand that to do this, they are connecting to the internet and using a search engine such as Purple Mash search or internet-wide search engines.	Children can collect, analyse, evaluate and present data and information using a selection of software, e.g. using a branching database (2Question), using software such as 2Graph. Children can consider what software is most appropriate for a given task. They can create purposeful content to attach to emails, e.g. 2Respond.	Children demonstrate the importance of having a secure password and not sharing this with anyone else. Furthermore, children can explain the negative implications of failure to keep passwords safe and secure. They understand the importance of staying safe and the importance of their conduct when using familiar communication tools such as 2Email in Purple Mash. They know more than one way to report unacceptable content and contact.

Year 4

	Information Technology		Digital Literacy
Statement	Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.	Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.	Use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concern about content and contact.
Outcome	Children understand the function, features and layout of a search engine. They can appraise selected webpages for credibility and information at a basic level.	Children can make improvements to digital solutions based on feedback. Children make informed software choices when presenting information and data. They create linked content using a range of software such as 2Connect and 2Publish+. Children share digital content within their community, i.e. using Virtual Display Boards.	Children can explore key concepts relating to online safety using concept mapping such as 2Connect. They can help others to understand the importance of online safety. Children know a range of ways of reporting inappropriate content and contact.

Year 5

	Information Technology		Digital Literacy
Statement	Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.	Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.	Use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concern about content and contact.
Outcome	Children search with greater complexity for digital content when using a search engine. They can explain in some detail how credible a webpage is and the information it contains.	Children can make appropriate improvements to digital solutions based on feedback and can comment on the success of the solution. e.g. coding to a design brief using 2Code. They objectively review solutions from others. Children can collaboratively create content and solutions using digital features within software such as collaborative mode. They can use several ways of sharing digital content, i.e. 2Blog, Display Boards and 2Email.	Children have a secure knowledge of common online safety rules and can apply this by demonstrating the safe and respectful use of a few different technologies and online services. Children implicitly relate appropriate online behaviour to their right to personal privacy and the mental well-being of themselves and others.

Year 6

		Information Technology		Digital Literacy
Statement	Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.	Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.	Use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concern about content and contact.	
Outcome	Children readily apply filters when searching for digital content. They can explain in detail how credible a webpage is and the information it contains. They compare a range of digital content sources and can rate them in terms of content quality and accuracy. Children use critical thinking skills in everyday use of online communication.	Children make clear connections to the audience when designing and creating digital content. The children design and create their own blogs to become a content creator on the internet, e.g. 2Blog. They can use criteria to evaluate the quality of digital solutions and can identify improvements, making some refinements.	Children demonstrate the safe and respectful use of a range of different technologies and online services. They identify more discreet inappropriate behaviours through developing critical thinking, e.g. 2Respond activities. They recognise the value in preserving their privacy when online for their own and other people's safety.	

### **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 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.

- 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/>



## 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)