



# Bingham Primary School

Policy Document

Policy Name: E-Safety Policy

Date: Sept 2024

Review: Sept 2025

*This policy makes reference to the 2019 document: 'Teaching online safety in school Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects'*

## **Introduction:**

At Bingham Primary School and Nursery ( to be known as BPSN for the rest of this policy) we recognise that in order to ensure our learners are well prepared for life in modern Britain, we need to equip them with the skills they need to make informed choices about themselves, their safety and also about how they behave towards others.

This includes the responsibility to teach all learners about how to navigate the online world, keeping themselves safe as well as ensuring they understand how to respect others.

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. We will aim to stay up to date with the latest devices, platforms, apps, trends and related threats.

Our aim is for our PHSE/RHSE and computing curriculums to continually evolve over time to reflect these changes as we believe it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

All our teaching must and will always be age and developmentally appropriate.

Our curriculum provision ensures that we are teaching about online safety and harms within a whole school approach.

Through our provision we always aim to:

- Create a culture that incorporates the principles of online safety across all elements of school life. These principles are reflected in wider whole school policies and practice. These are available and shared with staff, pupils and parents.

This policy therefore, should be viewed in conjunction with our whole school child protection policy which sets out clear processes for reporting incidents or concerns. There is also guidance about supporting pupils to understand acceptable online behaviours in the school's behaviour and bullying policies

It is our intention that through our curriculum teaching, Pupils will be just as clear about what is expected of them online as offline.



## Bingham Primary School

Policy Document

Policy Name: E-Safety Policy

Date: Sept 2024

Review: Sept 2025

We aim to be continually:

- Proactively engaging staff, pupils and parents/carers in school activities that promote the agreed principles of online safety.
- Reviewing and maintaining the school and curriculum online safety principles in line with changing information.
- Embedding the online safety principles when teaching curriculum subjects and other teaching opportunities. Teachers and all adults in school will reinforce what is taught in lessons by taking appropriate and consistent action when a pupil makes a report of unacceptable online behaviours from another pupil, including cyberbullying, or shares a concern about something they have seen online.
- Modelling the online safety principles consistently. This includes expecting the same standards of behaviour whenever a pupil is online at school - be it in class, logged on at the library or using their own device in the playground.

Through our website, information evenings and signposting to external agencies, we will ensure that we extend support to parents, so they are able to incorporate the same principles of online safety at home.

Teaching about online safety Underpinning knowledge and behaviours.

Underpinning knowledge and behaviours include:

**How to evaluate what they see online** - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

We will aim to help pupils consider questions including:

- is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

**How to recognise techniques used for persuasion** – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

We will aim to help pupils to recognise:

- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
- techniques that companies use to persuade people to buy something,
- ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and
- criminal activities such as grooming (at an age-appropriate level).

**Online behaviour** –Our pupils need to understand what acceptable and unacceptable online behaviour look like, from others online but also from themselves. We will aim to teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others.



## Bingham Primary School

Policy Document

Policy Name: E-Safety Policy

Date: Sept 2024

Review: Sept 2025

Our curriculum provision will support pupils to recognise unacceptable behaviour in others. We will help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- looking at how online emotions can be intensified resulting in mob mentality,
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

### Harms and risks

Understanding and applying the knowledge and behaviours above will provide pupils with a solid foundation to navigate the online world in an effective and safe way. However, we are very aware that we also need an understanding of the risks that exist online so our curriculum can continue to be evaluated and evolve, supporting our teachers to tailor their teaching and support to the specific contextual needs of our own pupils.

Some of the potential harms that our pupils might encounter at BPSN:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

**How to identify online risks** – This will enable our pupils to identify possible online risks and make informed decisions about how to act. We do not aim for this to be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Our curriculum and support can help pupils to identify and manage risk by:

- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,
- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?



## Bingham Primary School

Policy Document

Policy Name: E-Safety Policy

Date: Sept 2024

Review: Sept 2025

**How and when to seek support** – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We aim to help pupils by:

- helping them to identify who trusted adults are, both in school and outside of school.
- looking at the different ways to access support from adults in school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This links to our wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

### Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. We expect all our teachers to consider the most vulnerable pupils when planning their lessons from our curriculum. They will be expected to understand the nature of their pupils vulnerabilities and as a result, consider how they tailor their offer to ensure these pupils receive the information and support they need.

The following resources will support teachers when they consider how best to support their most vulnerable pupils stay safe online:

- Vulnerable Children in a Digital World - Internet Matters
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section
- STAR SEN Toolkit – Childnet

### Our E-Safety education will be provided in the following ways (this list is not exhaustive):

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in the ICT suite
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

### 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.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements set by the Trust and Nottinghamshire local authority.
- There will be regular reviews and audits of the safety and security of school ICT systems
- 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



## Bingham Primary School

Policy Document

Policy Name: E-Safety Policy

Date: Sept 2024

Review: Sept 2025

- All users will be provided with a username and password – these will not be shared with others and users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

All staff and pupils will be expected to follow the schools 'Internet Acceptable Use' Policy

### Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- 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.