Elburton Primary School

ONLINE SAFETY POLICY

This policy was adopted and ratified by the Full Governing Body of Elburton Primary School.

Date	Description
December 2023	Policy Agreed
December 2024	Review

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board
The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, ebulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs. If applicable, add: The governor who oversees online safety is Anna Clooke (Chair of Governors) All governors will:
- ❯ Ensure they have read and understand this policy
- ❯ Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- ❯ Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- ❯ Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher
The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

> ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

> Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

> Working with the trust IT Operations Manager to make sure the appropriate systems and processes are in place

> Working with the trust IT Operations Manager and other staff, as necessary, to address any online safety issues or incidents

> Managing all online safety issues and incidents in line with the school's child protection policy

> Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

> Updating and delivering staff training on online safety

> Liaising with other agencies and/or external services if necessary

> Providing regular reports on online safety in school to the headteacher and/or governing board

> Undertaking annual risk assessments that consider and reflect the risks children face

> Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Trust IT Operations Manager

The trust IT Operations Manager is responsible for:

> Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

> Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

> Conducting a full security check and monitoring the school's ICT systems

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

> Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here' This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:
- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:
- 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

Pupils in **Key Stage (KS) 2** will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

> Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:
> That people sometimes behave differently online, including by pretending to be someone they are not
> That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
> The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
> How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
> How information and data is shared and used online
> What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
> How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety
The school will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:
> What systems the school uses to filter and monitor online use
> What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying
6.1 Definition
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the effective behaviours policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

> Poses a risk to staff or pupils, and/or
> Is identified in the school rules as a banned item for which a search can be carried out, and/or > Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or a member of the senior leadership team.
> Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
> Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

> Cause harm, and/or
> Undermine the safe environment of the school or disrupt teaching, and/or > Commit an offence

If inappropriate material is found on the device, it is up to the headteacher or member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

> They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

› The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

› **Not** view the image
› Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

› The DfE's latest guidance on searching, screening and confiscation
› UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Elburton Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Elburton Primary School will treat any use of AI to bully pupils in line with our effective behaviours policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

› Lessons
› Break or lunch time
› Clubs before or after school, or any other activities organised by the school

All mobile devices must be handed to the class teacher at the beginning of the school day. These will be safely secured throughout the day and handed back to the pupil at the end of the school day.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

› Keeping the device password-protected
› Making sure the device locks if left inactive for a period of time

> Not sharing the device among family or friends
  Installing anti-virus and anti-spyware software
> Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from trust IT Operations Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on effective behaviour and ICT acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

By way of this training, all staff will be made aware that:

> Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
> Children can abuse their peers online through:
  o Abusive, harassing and misogynistic messages o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  o Sharing of abusive images and pornography, to those who don't want to receive such content
> Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:
- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

> Child protection and safeguarding policy
> Effective Behaviours policy
> Staff disciplinary procedures
> Data protection policy and privacy notices
> Complaints procedure
> ICT and acceptable use policy
> Anti Bullying and Harassment Policy

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

ELBURTON PRIMARY SCHOOL

STAFF AND VOLUNTEER ACCEPTABLE USE OF ICT POLICY AGREEMENT

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which provide new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe internet access. This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email, and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g., laptops, email, VPN etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use providing it does not affect the safety or efficiency of the school system.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on the school website/VPN) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal handheld/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- If the data on any device is breached, I will report it to the DPO and the Senior Leadership Team
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download, or access any materials which are illegal (child abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this does not affect the safety or efficiency of the computer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in Learning Academies Trust's Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. Paper based protected and Restricted data must be held in lockable storage. Any USB type devices which are which are used to take data off site e.g., homeworking must be on a password-protected encrypted device.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- If staff can access their school e-mails via home systems, laptops, or mobile phones/devices it is imperative that these are password protected to secure the relevant data and two-factor authentication is used.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school, and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I would be subject to disciplinary action. This could include a warning, a suspension, referral to local Governing Board, Learning Academies Trust Board, and in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name	
Signed	

Date	