



# Sebert Wood Primary School

## Online Safety Policy

**Date reviewed:** Autumn Term 2024

**Date to be reviewed:** Autumn Term 2026 *(or as and when required)*

**Approval by:** Headteacher

**Signature of**

**Headteacher:**

### 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

## 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](#)
- [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.

## Roles and responsibilities

### 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 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 the 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.

The governor who oversees online safety is Stephen Rusanen.

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)

### **The headteacher**

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

### **The Designated Safeguarding Lead (DSL)**

Details of the school's designated safeguarding lead (DSL) and alternates are set out in our child protection and safeguarding policy, as well as relevant job descriptions. One of the DSLs takes lead responsibility for online safety in school.

### **The Online Safety Lead**

The Online Safety Lead is responsible for:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and 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 ICT technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT technician 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 on CPOMS 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 organising staff training on online safety
- Liaising with other agencies and/or external services if necessary
- 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

### **The ICT technician**

The ICT technician 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 security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

### **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 2 and 3)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

### **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 2 and 3)

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](#)
- Parent resource sheet – [Childnet](#)

### **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).

## **Educating pupils about online safety**

All pupils will be taught about online safety as part of the curriculum.

In **Key Stage 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 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.

### **Educating parents/carers about online safety**

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

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.

### **Cyber-bullying**

#### **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 one

person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### **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 class groups, and the issues will be addressed in assemblies.

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 Training section 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 school behaviour 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.

### **Examining electronic devices**

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school's behaviour policy), 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.
- 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 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 DSL or other members 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.

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](#)
- Our behaviour policy

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

### **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.

Sebert Wood 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Sebert Wood will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed. They should review these tools in advance before using with pupils.

## 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.

## Pupils using mobile devices

Pupils in Years 5 and 6 may bring mobile devices to school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Sebert Wood has a separate policy about the use of mobile phones in school (The Mobile Phone and Wearable Technology Policy). This policy applies to staff and other adults, and to the use of pupils' mobile phones.

Although we do not expect pupils to bring mobile phones to school, we recognise some of our Year 5 and Year 6 pupils will be travelling to and from school independently so parents may wish them to bring one. There is an acceptable use agreement for pupils to sign when they start Years 5 and 6 (see The Mobile Phone and Wearable Technology Policy), with a copy sent home for parents to also review.

If the child brings a phone it must be switched off on arrival at the school site. It must be handed in at the start of the school day and will be stored securely until the end of the school day. The pupil is responsible for collecting the phone at 3.30pm and it must not be switched on again until they are leaving the school site. They may not be used during or after school clubs and activities. Phones may not be stored in coats, bags or lockers.

## Staff using work devices outside school

In the course of normal operations, ICT resources are to be used for business purposes only. Staff who have been given the use of a school laptop or iPad (and will be removing it from the premises) will be expected to sign for its use on receipt. Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite. The school

permits limited personal use of ICT facilities by authorised users. Staff may use school equipment for authorised business use under the following conditions:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- Personal use of the Internet must not involve attempting to access the categories of content described above.
- Passwords must be protected and account details must not be shared.

### **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 behaviour and acceptable use of computing/ICT (see appendices 2 and 3).

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 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.

### **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 and staff meetings).

The DSL and alternates will undertake child protection and safeguarding training, which will include online safety, at least every two 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.

## Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Keeping Children Safe in Education 2024
- Working Together to Safeguard Children 2019
- Whistleblowing policy
- Behaviour Policy
- Mobile and Wearable Technology Policy
- Staff code of conduct
- Guidance on Safer Working Practice 2022
- Teaching Online Safety in Schools DfE June 2019
- Information Management Handbook (including Confidentiality)
- Data Protection
- Prevent Strategy

## Appendix 1

### Acceptable Use of ICT Agreement for Staff, Governors, Volunteers and Visitors

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Use the school WIFI network on my personal device without permission from the headteacher or Online Safety Lead

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will not use social networking sites (on my own device or school's) to discuss school-related issues.

## Appendix 2

### Acceptable Use of Computing/ICT - Agreement for Children – Early Years & Key Stage 1

**For parents/carers:** Computing/Information Communication Technology (ICT), including using the internet, is an important part of learning in every school. At Sebert Wood, we use a filtered internet system but we expect all children to be safe and responsible users. Teachers explain the rules below to their class but please also read and discuss these with your child.

#### *Pupils' Acceptable Use of Computing/ICT Agreement*

*When I use the school's ICT systems (like computers) and get onto the internet in school I will:*

- *Ask a teacher or adult if I can do so before using them*
- *Only use websites that a teacher or adult has told me or allowed me to use*
- *Tell my teacher immediately if:*
  - *I select a website by mistake*
  - *I receive messages from people I don't know*
  - *I find anything that may upset or harm me or my friends*
- *Use school computers for school work only*
- *Be kind to others and not upset or be rude to them*
- *Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly*
- *Only use the username and password I have been given*
- *Try my hardest to remember my username and password*
- *Never share my password with anyone, including my friends.*
- *Never give my personal information (my name, address or telephone numbers) to anyone online*
- *Check with my teacher before I print anything*
- *Log off or shut down a computer when I have finished using it*

*I agree that the school will monitor the websites I visit and understand that there will be consequences if I don't follow any of these rules, which could include not being allowed to use school computing equipment.*

### Appendix 3

#### Acceptable Use of Computing/ICT - Agreement for Children – Key Stage 2

**For parents/carers:** Computing/Information Communication Technology (ICT), including using the internet, is an important part of learning in every school. At Sebert Wood, we use a filtered internet system but we expect all children to be safe and responsible users. Teachers explain the rules below to their class but please also read and discuss these with your child.

#### Pupils' Acceptable Use of Computing/ICT Agreement

*When I use the school's ICT systems (like computers) and get onto the internet I will:*

- *Always use the school's ICT systems and the internet responsibly and for educational purposes only*
- *Only use them when a teacher is present, or with a teacher's permission*
- *Keep my usernames and passwords safe and not share these with others*
- *Keep my private information safe at all times and not give my name, address or telephone number to anyone online*
- *Tell a teacher (or another adult) immediately if I find any material that might upset, distress or harm me or others*
- *Always log off or shut down a computer when I've finished working on it*

*I will not:*

- *Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity*
- *Use any inappropriate language when communicating online*
- *Create, link to or post any material that is offensive, obscene or otherwise inappropriate*
- *Log in to the school's network using someone else's details*
- *Open someone else's school files*
- *Bring any memory sticks or other storage devices into school (unless I have the permission from a teacher)*

*I agree that the school will monitor the websites I visit and understand that there will be consequences if I don't follow any of these rules, which could include not being allowed to use school computing equipment.*