

# Waterbeach Community Primary School



## Online Safety Policy

Date approved by Governors: February 2023

Date for review: February 2024

Source: Local Authority

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.

# Online Safety Policy

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Department'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.

## 3. Roles and responsibilities

### 3.1 The governing body

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

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on Acceptable Use Agreement.

### 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 DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.

Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

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

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately

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 body

### **3.4 The ICT Service**

The ICT Service is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 on a regular basis

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 (reported by the ICT school technician)

### **3.5 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

Implementing this policy consistently

Agreeing and adhering to the terms on Staff Acceptable Use Agreement by signing the attached form.

Ensuring that pupils follow the school's terms on acceptable use.

Working with the DSL/IT Technician to ensure that any online safety incidents are reported and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately.

### **3.6 Parents**

Parents 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 Agreement

Parents 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 factsheet - [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.

## **4. Educating pupils about online safety**

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

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.

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

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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 5. Educating parents about online safety

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

If parents 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 one person or group by another person or group, where the relationship involves an imbalance of power.

### 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.

Teaching staff are 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).

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### **6.3 Examining electronic devices**

In line with our Acceptable Use Agreement, children should not normally bring devices into school.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

## **7. Acceptable use of the internet in school**

The Acceptable Use Agreements are shared with all pupils, parents, staff, volunteers and governors. 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.

## **8. Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of Acceptable Use Agreement.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Work devices must be used solely for work activities.

## **9. How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, 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 and or 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 which involve illegal activity or content, anything relating to the Prevent Duty or otherwise serious incidents, should be reported to the police.

## **10. Training**

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.

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.

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.

## **11. Monitoring arrangements**

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

This policy will be reviewed every 2 years or when there are local/ National updates. At every review, the policy will be shared with the governing body.

## **12. Links with other policies**

This online safety policy is linked to our:

Child Protection and Safeguarding Policy

Behaviour Policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Acceptable use agreements – KS1, KS2, Staff, Community users

Our school encourages each child to grow into a happy, confident individual, thriving in a supportive community where each is inspired to learn and discover through a kaleidoscope of opportunities, with space to imagine and to create.