



WALKERINGHAM  
PRIMARY SCHOOL

think smart be kind

# Online Safety Policy

Reviewed: Spring 2026  
Next Review: Spring 2027

## **CONTENTS:**

1. Policy Development
  2. Teaching and Learning
  3. Managing Internet Access
  4. Policy Decisions
  5. Communicating the policy
  6. Appendices
- 

### **1. Policy development**

The online safety policy is part of the School Development Plan and relates to other policies including those for Information & Communications Technology (ICT), Anti-bullying and Safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office

#### **Roles and responsibilities**

Mr Luke Scoffield, Head Teacher has responsibility for online safety.

### **2. Teaching and Learning**

#### **Why internet and digital communications are important**

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. There is a link to Child Exploitation and Online Protection (CEOP) on the school website.

- Issues such as Cyberbullying and online safety will be built into the curriculum to encourage self-efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

### **3. Managing Internet Access**

#### **Information security system**

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority and Walkeringham Primary School's IT provider (Orchestrate IT).

#### **E-mail**

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a school learning platform (Teams) and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

#### **Published content and the school website**

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published
- The headteacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

#### **Publishing pupils' images and work**

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified. Group photographs will be used rather than full-face photos of individual children, unless authorised by parents.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission, via the data capture sheet issued at the beginning of the school year, will be obtained from parents and carers before any photographs are published on the school website, social media, TV, other external sources, school promotional materials, class and school dojo pages.

#### **Social networking and personal publishing on the school learning platform**

- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

### **Managing filtering**

- The school will work with their IT provider (Orchestrate IT) to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the online safety coordinator
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

### **Managing Teams/Zoom/Videointerferencing and remote learning**

- Walkeringham PS will only use the Microsoft TEAMS or Zoom for video conferencing activity and will only use approved or checked webcam sites.
- In response to closure of schools and need to provide a home learning platform, staff will be using the two platforms to provide whole/group class sessions for the children.
- The above will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving the above calls.
- The above platforms will use the educational broadband network to ensure quality of service and security.

### **Class Dojo**

- Photographs that include children will be selected carefully to be added to the child's personal story or class story depending on permissions.
- Parents are asked if they want to link to their child's account so they can see what is happening inside our classrooms and schools and so children can share their learning at home.

#### *Promises Class Dojo make:*

- *We don't share any of your information or students' information with advertisers or marketers.*
- *We don't own anything you add to Class Dojo: you do.*
- *Students' portfolios are private to the classroom.*
- *We use the latest security best practices to protect you at all times.*
- *We are compliant with COPPA, FERPA, and GDPR in Europe.*
- *We will notify you if we make any changes to our practices*

### **Managing emerging technologies**

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

### **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **4. Policy decisions**

### **Authorising internet access**

- All staff must read and sign the 'staff code of conduct before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form
- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site

### **Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the online safety policy is appropriate and effective.

### **Handling online safety complaints**

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the headteacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

### **Community use of the internet**

- All use of the school internet connection by community and other organisations shall be in accordance with the online safety policy.

## **5. Communicating the policy**

### **Pupils**

- Appropriate elements of the online safety policy will be shared with pupils.
- Online safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of online safety. These will be addressed on a regular basis and modified as newer risks are identified.

### **Staff**

- All staff will be informed of the online safety policy and required to sign 'acceptable use of school ICT resources' to acknowledge that they have read and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.

- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting.

### **Parents**

- Parents will be notified of the policy in newsletters, the school brochure and website
- All parents will be asked to sign the parent/pupil agreement when they register their children.
- Parents will be offered online safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely via the following online platform which is available on the parents page of the school website:  
<https://www.childnet.com/parents-and-carers/parent-and-carer-toolkit>

## **6. Appendices**

### **Appendix 1**

#### **The Legal Framework**

##### **Communications Act 2003(section 127)**

Sending by means of the internet a message or other matter that is offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction to imprisonment.

NB an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

##### **The Computer Misuse Act 1990**

Regardless of an individual's motivation, the act makes it a criminal offence to:

- Gain access to computer files or software without permission
- Gain unauthorised access as above in order to commit a further criminal act
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

##### **Copyright, Design and Patents Act 1988**

Copyright is the right to prevent others from copying or using work without permission.

##### **Data Protection Act 1998**

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data.

##### **Education Act 2011 (sections 2-4)**

This clarifies statutory powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. Details for free schools can be found in section 36 and Academies in part 6 sections 55-65.

##### **Education and Inspections Act 2006 (sections 90-91)**

This provides powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. It also gives schools the powers to confiscate items from pupils.

These powers are particularly relevant to online bullying and online safety as well as giving legal powers to confiscate mobile phones and other mobile devices, if they suspect that they are being used to compromise the well-being and safety of others.

##### **Malicious Communications Act 1988 (section1)**

This makes it a criminal offence to send electronic messages that conveys indecent, grossly offensive, threatening material or information that is false. This includes if the message is of an indecent or grossly offensive nature and if the purpose was to cause a recipient to suffer distress or anxiety.

### **Obscene Publications Act 1959 and 1964 (section 1)**

Publishing an 'obscene' article is a criminal offence. This includes electronic transmission.

### **Public Order Act 1986 (sections 17-29)**

This makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. It also makes the possession of inflammatory material with a view of releasing it a criminal offence.

### **Protection of Children Act 1978 (section 1)**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the UK. A child is anyone under 18. Viewing an indecent image of a child on your computer means that you have made a digital image.

### **Protection from Harassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which they know or ought to know amounts to the harassment of others.

A person whose course of conduct causes another to fear on at least 2 occasions, that violence will be used against them is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear on each of these occasions.

### **The Equality Act 2010**

This consolidates discrimination law covering all types of discrimination that are unlawful. It defines that schools cannot unlawfully discriminate against pupils because of their sex, race, disability, religion or belief and sexual orientation. Protection is now extended to pupils who are pregnant or undergoing gender reassignment.

### **Regulation of Investigatory Powers Act 2000**

This regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication.

The Telecommunications (Lawful Business Practice) (Interception of Communications Regulations 2000) does permit a degree of monitoring and record keeping for example in schools to investigate unauthorised use of the network. However all monitoring is subject to consent.

### **Sexual Offences Act 2003**

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice and intentionally meet them or travel with the intent to meet them to commit a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Any sexual intercourse with a child under 13 is considered rape.

## Appendix 2

### **Walkeringham Primary School ICT Acceptable Use Policy for: All staff/governors/visitors/volunteers**

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my user name.
- I will only use the school email, internet, intranet, Learning platform or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the headteacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the e-safety coordinator, the Child Protection Officer or the head teacher
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

#### **User Signature**

I agree to follow the code of conduct and support the safe use of ICT throughout the school

Full Name: \_\_\_\_\_