Online Safety Policy

Approved by Governors	**4th December**
Written	**December 2024**
To be reviewed	**December 2025 (or in light of new legislation)**

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Worsthorne Primary School embraces the positive impact and educational benefits thatcan be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Worsthorne Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Our Online Policy, as part of the wider safeguarding and Child protection agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

Our Vision

Worsthorne Primary School's vision for Online Safety is to provide a diverse, balancedand relevant approach to the use of technology. Our pupils will be encouraged to maximise the benefits and opportunities that technology has to offer by following the guidelines in the Lancashire Primary Online Safety framework. We will ensure that children will learn in a safe andsecure environment so that they can learn effectively. Our aim is that pupils will be equipped withthe skills and knowledge to use 21st Century technology appropriately and responsibly. Pupils will be taught how to recognise the risks associated with this technology and how to deal with them, both inside and outside the school environment.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

The role of the school's Online Safety Champion

Our Online Safety Champion is Michelle Kayley and the Headteacher for Safeguarding and Child Protection.

The core duties/role of the Online Safety Champion includes:

- Operational responsibility to ensure the development, maintenance and review of the school policy and associated documents, including Acceptable Use Policies.

- Ensure that the policy is implemented and that compliance with the policy is actively monitored.
- Ensure all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensure the Online safety Incident Log is appropriately maintained and regularly reviewed.
- Keep personally up to date with Online Safety issues and guidance through liaison with Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- To provide or arrange Online Safety advice/training for staff, parents/carers and governors.
- Ensure that SLT, staff, pupils and governors are updated as necessary.

Publicising Online -Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website
- Introduce this policy, and related documents, to all staff at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant Online Safety information in all areas where computers are used
- Provide Online Safety information through the school newsletter

Policies and practices

The Online Safety policy should be read in conjunction with the following other related policies and documents:

- Anti-Bullying Policy
- Computing Policy
- Behaviour Policy
- Safeguarding and Child Protection Policy

Security and Data Management

This section of the policy offers clear guidance to users regarding the management of potentially sensitive data.

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be;

- Accurate
- Secure
- Fairly & lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection

In our school, data is kept secure and all staff are informed as to what they can and cannot do with regard to data in the following ways:

- The person responsible for managing information in school is the School Business Manager Ms. Jo. Hanson
- Relevant staff know the location of data
- Staff with access to personal data understand their legal responsibilities
- School will ensure that data is appropriately managed both within and outside the school environment
- All staff are aware that they should only use approved means to access, store and dispose of confidential data
- Staff who have remote access to school data must ensure the data remains secure by being aware of the dangers of unsecured wireless access outside school

Mobile devices and removable media

- Data held on mobile devices and removable media is password protected and encrypted
- Devices containing data may be allowed to be removed from the school premises with the knowledge of the Headteacher/School Business Manager
- Staff are aware that personal devices must not be used to access data on school systems, such as downloading e-mail or files to a Smartphone
- LCC Digital Services ensures the risk of admin data loss is addressed and managed
- Day to day monitoring of our system back-up is undertaken remotely by Educational Digital Services.
- Pupils, parents/carers and visitors will not be permitted to use any mobile device on the classroom floor or in any areas where there are children.

Use of mobile devices

In our school we recognise the use of mobile devices and removable devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- Staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content
- Permanent staff are permitted to access guest Wi-Fi using their personal devices. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below. School will ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media and consider the purpose for which the image will be used e.g. school website or display. As photographs and video of pupils and staff are regardedas personal data in terms of The Data Protection Act (1998), school will obtain written permissionfor their use from the individual and/or their parents or carers.

- Permission will be obtained from parents/carers upon the pupil entering the school. Permission is given for 5 years.
- School will not re-use any photographs or videos after 5 years of consent without further consent being sought.
- Full names and personal details will not be used on any digital media, particularly photographs
- Parents/carers who have been invited to attend school events and allowed to take photographs and videos, will be made aware of any conditions prior to the event in writing or verbally at the event.
- Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Networking sites.
- Staff are aware that photographs/video that are taken using school equipment must only be used for school purposes, and only accessible to the appropriate staff/pupils.
- Staff must not use their own personal media devices to take photographs or videos.
- When taking photographs/video staff will ensure that all subjects are appropriatelydressed and not participating in activities that could be misinterpreted
- Staff, parents/carers and pupils will be educated in the dangers of publishing images and videos of pupils or adults on Social Networking sites or websites without consent of the persons involved
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy will be monitored annually by the Online Safety Champion.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated daily
- Central filtering is provided and managed by Netsweeper with filtering via Digital Educational Services. All staff and students understand that if an inappropriate site is discovered it must be reported to Sarah Nicholls who will report it to Educational Digital Services to be blocked. All incidents will be recorded in the Online Safety log for audit purposes.
- Requests for changes to the filtering will be directed to Educational Digital Services. The school uses Sophos Virus protection and central blocking on all school owned equipmentto ensure compliance with the Acceptable Use Policies.
- Pupils use is monitored
- Staff use is monitored by the Head
- All staff are issued with their own username and password for network access. Students use class log-ins, which have restricted access to our server.
- Any visitors (including consultants, creative practitioners) who wish to display material in school via interactive whiteboards/screens may do so in two ways:

    1. Connect via their own laptop via a VGA lead to the whiteboard

    2. Email material to Sarah Nicholls who will make it available on our server

    NB. External hard drives and pen sticks are not to be used on our PCs and laptops

- A 'guest' log-in is available for use of our internet facility for supply staff/ visitors

- Pupils are issued with a device number

Communication technologies

Email

In our school the following statements reflect our practice in the use of email.

All staff have access to the Office 365 as the preferred school e-mail system & this is used for any work related activity

- Only official email addresses are used to contact staff
- Only key named staff are permitted to manage confidential information
- E-Mail communication is routinely monitored in accordance with Acceptable Use Policy
- Incidents of SPAM are reported to the Headteacher
- Threatening or offensive e-mails are reported to the Online Safety Champion & evidence collected
- Pupils do not have individual e-mail accounts. If required as part of curriculum work, teachers create class accounts (within specific closed environment software packages) & manage these for the duration of a project, after which they are closed.

In our school the following statements outline what we consider to be acceptable and unacceptable use of the following:

Mobile telephones

- Pupils may at times bring mobile devices into school but these must be stored in the baskets in each class which are then stored in a locked cupboard. Children are not permitted to use them during lessons, clubs before or after school, or any other activities organised by the school.

Instant Messaging

- Pupils to have no access to Instant messaging. If the curriculum required, it would only be as a part of carefully planned school activities (and with Head teacher permission) and under direct control of the teacher, as a class learning tool.

Web sites and other online publications

- The school website is managed & monitored by a key named member of staff.
- Content uploaded to the website is carefully controlled to ensure high levels of security and adherence to AUP requirements.
- All staff are aware of the importance of ensuring online safety when submitting items for publication on the school website.
- Pupils' work is not displayed in other digital locations

Video conferencing

- Teams is the preferred video conferencing tool as it is easily accessible and straightforwardto set up.
- Video conferencing will only take place as part of carefully planned and approved education projects (with Headteacher permission).
- Parental written consent will be secured before video conferencing is undertaken.
- Teachers will be directly responsible for managing video conferencing sessions.
- Under no circumstances will children undertake video conferencing independently.
- Video conference partners will be carefully and systematically vetted to ensure pupil safety(e.g. use of trusted sources – schools, museums, education departments).
- Written and signed agreements will be in place prior to video conferencing sessions in order to ensure preservation of copyright, privacy and Intellectual Property Rights (IPR).
- Full training for staff will be provided prior to commencing video conferencing activities.
- Video conferencing will be managed by a teaching team, not individual staff.

Acceptable Use Policy (AUP)

The school actively promotes responsible, safe & courteous behaviour when accessing and using technology. Issues such as internet safety, copyright, plagiarism, cyberbullying & respect

for others' work are addressed regularly as a part of ongoing class projects. Staff act as positive rolemodels and trusted adults and have signed AUP agreements.

The school has adapted the Lancashire AUP template agreement format for future AUP policy development, modification and use.

Dealing with incidents

Incident Log

The school records and monitors any incidents/offences in relation to online safety via CPOM's (our school Safeguarding record keeping platform) and it is audited on a regular basis by the Online Safety Champion/DSL/safeguarding Governor.

Illegal Offences

Any suspected illegal material or activity will be brought to the immediate attention of the Headteacher and referred to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF) who will take responsibility for all aspects of investigation. The school recognises the importance of following correct procedures and will not conduct investigations independently.

Inappropriate Usage

Accidental access to inappropriate materials occurs very rarely and children and adults are aware of the necessary actions to take (minimise webpage, turn monitor off and tell a trusted adult immediately). The adult will then inform Sarah Nicholls and log the incident on CPOMS using the 'online' category. These procedures are regularly reinforced as an integral part of ICT sessions. Details will be entered on CPOM's and reported to Educational Digital Services if necessary.

Infrastructure and Technology

The school provides and maintains an infrastructure and network that offers high levels of security.

Pupil Access

Pupils are only permitted to access the internet and school network as part of their studies. Teaching staff and Assistants are always present during periods of internet and network use. Where possible, selected sites are identified for pupil use and specific monitoring takes place when children navigatethe internet more freely. Automatic filtering is in place. Children are reminded regularly about theneed to be safe on line. This is a key feature of computing sessions containing on-line aspects.

Passwords

The school network is password protected. Staff have individual logins. Pupils gain access through class logins. Passwords are periodically reviewed and changed.

Software/Hardware

Software used in school is fully licensed and documentation is housed in secure on-site locations. TheBusiness Manager, Jo Hanson, retains licences for education software. ICT hardware and software are audited annually.

Managing the network and technical support

The network is managed by key named staff and a representative from the LCC Digital (service level agreement). Servers, wireless systems and cabling are securely located and physical access is restricted. All wireless devices are security enabled and are only accessible through use of secure passcode logins. Security on the network is managed by key named staff with support from LCC Digital Services. Review of safety and security is ongoing and critical updates automatically programmed to activate as required. Network users have clearly defined access rights. Permissions are assigned by key named staff.

All pupils and staff are aware of the need to follow routines in order to preserve network security. On completion of work, users log out and automatic lockdown facilities are activated to protect thenetwork if machines are inadvertently left unattended.

All software is installed using only Administrator login and permissions. Staff are permitted to transfer school work files to the network from portable hard drives and these are automatically scanned for viruses upon connection. Staff are aware of procedures to follow if they believe that security has been breached (key named points of contact).

All teachers have a school laptop. They are aware that this is school property and can be used both on-site and at home expressly for management and teaching purposes. They are not permitted to installadditional software without permission and personal files are not to be transferred to or stored onthis equipment. Teachers should use only school authorised equipment in school.

Filtering and virus protection

The school subscribes to the Lancashire Grid for Learning/LCC Digital Services broadband and high level internet content filtering is provided by default. Sophos Anti-Virus software is included in the school's subscription and this is configured to receive regular updates. On rare occasions, unsuitable content may get past the filter and pupils are taught to follow set procedures if this occurs (report instantly to staff and turn off monitor).

Education and Training

Online Safety across the curriculum

It is vital that pupils take responsibility to their own Online Safety. School will provide suitable online safety education to all pupils by considering the following:

- Regular, planned discreet Online Safety teaching using planning and resources from 'Purple Mash' scheme of learning

- Additional focus on Online Safety during the National Online Safety Awareness Week
- Online Safety education will be differentiated for pupils with SEND
- Pupils are made aware of the impact of Cyberbullying during both National Online Safety Week and National Anti-bullying Week by teachers. Pupils are advised how to seek help if they are affected by these issues
- Pupils are reminded of safe internet use by classroom displays and Online Safety rules

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 otheronline technologies

Pupils in Key Stage 2 will be taught to:

Use technology safely, respectfully and

responsiblyRecognise 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 reportthem

How to critically consider their online friendships and sources of information including awareness of the risks associatedwith 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 donot 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 alsoinvite speakers to talk to pupils about this.

Online Safety – Raising staff awareness

- A planned formal Online Safety training for all staff takes place annually to update them on their responsibilities outlined in this policy and the schools' Computing policy
- Headteacher/Online Safety Champion will attend training (from a county provider/CEOP) as and when required in order that they can provide advice/guidance or training to individuals
- Staff are made aware of issues which affect their own personal safeguarding e.g. use of Social Networking sites. NO staff member can accept an invite from any pupil past or present to 'add' them on to their friend contacts
- Staff are expected to promote and model responsible use of ICT and digital resources
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand the school's Online Safety Policy and the Acceptable Use Policy (AUP)
- Regular updates on Online Safety Policy, AUP, curriculum resources and general Online Safety issues are discussed in staff/team meetings

Online Safety – Raising parents/carers awareness

'Parents/Carers often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report, 2008)

School will offer regular opportunities for parents/carers to be informed about Online Safety. These will include the benefits and risks of using various technologies. School will do this by:

- School newsletters and school website,
- Promote external Online Safety resources/online materials as a handout to all children at National eSafety Week and thereafter.
- We subscribe to Knowsley City learning Centre who support school by providing Online Safety support through weekly Online Safety newsletters and offer Online Training for staff, parents and governors.

Online Safety – Raising Governors' awareness

Governors with specific responsibilities for Online Safety, ICT, Child Protection and Safeguarding Children and Anti- Bullying will be required to keep themselves up to date. This may be through discussion at Governor meetings, attendance at Local Authority or staff/parent/carer meetings. Our Online Safety Governor is Mrs. Amy. Angus.
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).

The governor who oversees online safety is

Mrs. Amy Angus

All governors will:

- Ensure that 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.

Standards and Inspection

Greater emphasis must be placed on monitoring child protection and safeguarding procedures within our school as technology is moving forward at such a rapid pace. School will consider the following to encompass this by ensuring:

- Online Safety incidents are monitored, recorded and reviewed (see appendix 10)
- New technologies are risk assessed & that they are included in the Online Safety Policy where appropriate
- Online Safety Champion to make necessary any changes to this policy, following regular reported Online Safety incidents which may affect practise within school
- Online Safety Champion to make staff, parents/carers, pupils and governors informed of any changes to policy and practice throughout the school year by use of class computing lessons, school newsletter/website, staff/governor meetings.