Healthy Empowered Ambitious Respectful Together

Our values are at the HEART of our school

Online Safety Policy

Policy Author:	Lauryn Tweedy
Date of Policy Review:	January 2025
Date approved by Governors:	January 2025
Next Review Date:	January 2028

Aims

This policy outlines Washingwell Primary Schools commitment to ensuring the safety of pupils, staff and the wider school community in the digital world. It applies to all individuals accessing school systems, devices and networks, both on-site and remotely, including staff, pupils, governors, parents, and visitors. Our school is committed to creating a safe and positive online environment for everyone and we achieve this by:

Protecting: Actively promoting and safeguarding the online safety of our pupils, staff, volunteers, and governors.

Educating: Equipping all members of our school family with the knowledge and skills to navigate the digital world safely and responsibly.

Empowering: Foster a culture of open communication and reporting, enabling early intervention and resolution of any online safety concerns.

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

● DfE's guidance on protecting children from radicalisation.

Washingwell Community Primary School's Online Safety Policy operates in conjunction with other policies and guidance:

- Behaviour and Exclusions
- Anti-Bullying
- Curriculum
- Data Protection
- Safeguarding Children in Education
- PREVENT
- Use of social media
- Health and Safety
- Home School Agreement

The school will monitor the impact of the policy using:

- Logs of reported incidents recorded on CPOMS
- Monitoring logs of internet activity (including sites visited) and filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of students, staff and parents

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team

effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the governor responsible for safeguarding. The role of the online safety governor will include:

- Ensure an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders
- Ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive
- Ensure that procedures for the safe use of ICT and the internet are in place and adhered to
- Hold the Head Teacher and staff accountable for online safety.

The Head Teacher

The Head Teacher 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 DSL and deputies are set out in our child protection and safeguarding policy.

The Computing Leader and DSLs take 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
- Working with the headteacher, computing technician, and other staff, as necessary, to address any online safety issues or incidents
- 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 This list is not intended to be exhaustive.

The Computing Technician

Washingwell Primary School works alongside Omnicom (our IT provider). The computing technician 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 IT 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 IT systems on a monthly basis

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

School Business Manager

Our School Business Manager is responsible for:

- Checking Securus, which is our schools filtering system, weekly and if any alerts occur, these are reported to the Subject Lead/Class teacher so appropriate action can be taken
- 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

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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- 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

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 of the school's IT systems and internet

Learners

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Visitors and Members of the Community

Visitors and members of the community who use the school's IT 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.

Why is Internet Use Important?

The purpose of Internet use in school is to raise education standards, to promote pupil achievement, to support the professional work or staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

Pupils will use the internet outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How can Internet Use Enhance Learning?

- The school internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not, and they are given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research including the skills of knowledge location, retrieval and evaluation
- Pupils will regularly learn about online safety across the Computing and PSHE curriculum.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents are informed that pupils will be provided with supervised internet access.
- Parents are asked to sign and return a consent form for pupil internet access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the School Business Manager or Head Teacher immediately.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Artificial Intelligence (AI)

Although pupils do not directly use AI tools in school, we recognise that artificial intelligence is increasingly present in the digital world children are growing up in. As part of our computing and digital literacy curriculum, pupils are taught what AI is, how it works in simple terms, and how to use it safely and responsibly.

Children are made aware of which apps and websites include AI features so that they can recognise and understand when they are interacting with AI. This helps them to become more aware of how AI functions are built into many online platforms and services. Pupils may encounter AI through educational tools such as **Scratch** and **Canva for Education**, where features like

automated design suggestions or coding assistance may be present. Staff ensure that any use of AI within these platforms is appropriate, age-appropriate, and closely supervised.

Email

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication.
- Whole class or group email addresses should be used in school.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking – see Use of Social Media Policy

- Access to social networking sites and news groups is prohibited unless a specific use is approved by Head Teacher.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them of their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised and instructed how to block unwanted communications. Pupils encourages to invite known friends only and deny access to others.

Filtering

- Washingwell Primary School works in partnership with Omnicom (IT provider) to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should not use mobile phone to take picture of videos of children – only ipads or digital cameras provided by the school are acceptable for this purpose.
- Mobile phones are not permitted to be used anywhere in school, around the children. Mobile phones may be used in office areas or the staff room. The only exception for this is staff taking a mobile phone with them on a school visit outside of school, for use in emergencies only. Children who bring mobile phones to school (only those in Year 5 or 6 who are walking home themselves) are required to hand them in to the class teacher and collect them at home time,

The PREVENT Duty and Online Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in school. We have an important role to play in equipping children to stay safe online. Internet safety is integral to our computing curriculum. Staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the wellbeing of any pupil is compromised.

Published Content and the School Website

The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

Written permission from parents or cares will be obtained before photographs of pupils are published on the school website and social media (Facebook). The consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/cares may withdraw permission, in writing, at any time.

Pupil's full names will not be used anywhere on the school website or Facebook, particularly in association with photographs.

Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs Taken by Parents/Carers for Personal Use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc. The consent form that parents sign at the beginning of their child's time at Washingwell states '*We do not wish to prohibit parents from capturing special memories however if you wish to video or photograph you child during school events, you must be aware that they cannot be shared on any open forums or websites, and are for personal use only. Please be aware that other parents may prosecute you personally if you have displayed imaged of their child without their consent'.*

Information System Security

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be organised by Omnicom (IT provider).

Protecting Personal Data

Personal data will be recorded, processed transferred and made available according General Data Protection Regulations. See also Data Protection Policy.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer, therefore, neither the school nor Omnicom can accept liability for material accessed, or any consequences of internet accessed. The school regularly audits IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate.

Handling Online Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedure.

- Pupils and parents will be informed of the complaint's procedure. **See also Complaints Policy.**

Communication of Policy

Pupils

- Rules for internet access will be posted in all networked rooms.
- Pupils are informed that internet use will be monitored.

Staff

- All staff will be given the School Online Safety policy and its importance explained.
- All staff will be trained in safeguarding procedures, including elements of Online Safety and The PREVENT Duty
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the schools Online Safety Policy in newsletters, the school prospectus and on the school website. The school will also organise online safety workshops to support parents understanding of how to best safeguard their children against potential online danger.

Community

- External organisations using the school's IT facilities must adhere to the Online Safety Policy.

Monitoring

Washingwell Primary School subscribes to the use of Securus – an internet use monitoring software tool. Securus is checked and managed by the School Business Manager. Any online safety incidents are reported the Head Teacher.

Appendix 1: Pupil Guidelines for Safe Internet / Email Use

Appendix 2: Internet Acceptable Use Agreement for Staff

Appendix 1

Washingwell Primary School
Internet Acceptable Use Arrangement for Pupils

I will only use the internet when there is a teacher present.

I will always ask for permission before accessing the internet or email.

I will only use my own usernames and passwords to log onto the system/email and keep them secret.

I will not access other people's files.

I will only email people I know, or who my teacher has approved and ensure that messages that I send are polite and responsible.

I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using the internet email etc.

I will not give personal details (like my home address, telephone or mobile number0, or the personal details of any other person to anyone, or arrange to meet someone under any circumstances.

I will only download, use or upload material when I have been given the owner's permission.

I will only view, download, store or upload material that is lawful an appropriate for users. If I am not sure about their, or come across any potential offensive materials, I will inform my class teacher straight away.

I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.

I will always quote the source of any information gained from the internet i.e. the web address, in the documents I produce.

I will use the internet for research and school purposes only.

I will not bring I memory sticks from home to use in school unless I have been given permission by my class teacher.

I understand that the school may check my compute files, emails and will monitor the internet sites that I visit.

I understand that if I do not follow these rules, my access to the school computer system/internet will be suspended and my parents/carers will be informed.

Appendix 2

Washingwell Primary School
Internet Acceptable Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Acceptable Use Agreement has been drawn up to protect parties – the students, the staff and the school.

Staff requesting internet access should sign a copy of this Acceptable Use Agreement statement and return it to the School Business Manager for approval.

- All internet activity should be appropriate to staff professional role or student's education.
- Access should only be made via the authorised account password, which should not be made available to any other person.
- Activity that threatens the integrity of the school IT system, or activity that attacks or corrupts other systems, is forbidden.
- Installation of software or hardware is not acceptable unless permission is sought from the Head Teacher.
- Users are responsible for all emails sent and contacts made that may result in emails being received.
- Staff should not use personal email accounts for school business. All staff and Governors have an @washingwell.org.uk email account set up for this purpose.
- Use for financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected at all times.
- Posting anonymous messages and forwarding chain letter is forbidden.
- As emails can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Us of the school network to access inappropriate materials such as pornographic, racist, homophobic or offensive material is forbidden.
- Staff will promote online safety with pupils in their care and help them to develop a responsible attitude to system use and to the content they have access to or create.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of email and deletion of inappropriate materials where it believes

unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I agree to abide by the internet acceptable use agreement detailed above throughout my time of employment at Washingwell Primary School	
NAME	
DATE	
SIGNED	