WESTFIELD PRIMARY SCHOOL

Online Safety Policy

This Policy was reviewed by K Beattie

January 2026

Review: January 2027

Online Safety, Safeguarding and Child Protection Lead:	Julia Findlay (DSL)
Online Safety Lead:	Kate Beattie
Status & Review Cycle:	Annual
Next Review Date:	January 2026

Online Safety Policy

Westfield Primary School promotes a culture where pupils feel confident to report concerns, knowing they will be taken seriously and supported.

This policy is written with reference to guidance from Keeping Children safe in Education 2025, which can be found here:

https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf

This policy also refers to the DFE advice and support on use of AI in schools, which can be found here:

https://www.safeguardinginschools.co.uk/dfeai

Why Internet and digital communications are important

- At Westfield we understand that the Internet is an essential element of 21st century life for education, business and social interaction. Therefore, the school has a duty to provide students with a high-quality understanding of the risks and benefits of spending time online, and equip them with clear strategies and understanding of managing themselves online and protecting themselves from harm.
- Internet use is a part of the statutory curriculum and a necessary, useful tool for staff and pupils.
- Pupils will be taught about the positives of the internet and how to protect themselves while using it. Teaching at Westfield centres around the 4Cs of online harms.

KCSIE 2025 categorises online harms into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Details of how these are covered in our Online Safety teaching can be seen in more detail in our progression and rationale of Computing teaching at Westfield. Teaching of Online Safety uses the Project Evolve (developed by SWGFL) being used across all year groups. This is supplemented by a wealth of online resources recommended by the DfE.
Reception – Smartie the Penguin
Year 1 - Digiduck
Year 2/3 – Jessie and Friends and Lee & Kim
Year 4 – Play like Share
Year 5 & 6 – Google internet legends.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught about the specific risks of live streaming, image-based abuse, pressure to share images, and the creation or distribution of AI-generated or edited images. They are taught that sharing sexual images of children is illegal, even if the image is of themselves.

<u>Internet Access</u>

- The school Internet access is an FTTP service provided by Schools Broadband and supported by Eduthing and includes filtering & security appropriate to the age of pupils and a Fortinet Firewall.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

The Victorians	Space	The Vikings
Autumn	Spring	Summer
Click the Sprite Scratch based game Children create a levelled game where players have to click on different items in order to earn points. **Online Reputation** **Online Relationships**	**Stop Motion** Children look at how you create a stop motion animation, learn the technical vocabulary and develop their own short films. **Privacy and Security** **Self Image and Identify**	**Google Slides** Children create presentations using animations, transitions and dictation about the Vikings **Managing Online Information** **Copyright and Ownership**

This details where the modules take place throughout the year. We look at activities from 'Health Wellbeing and Lifestyle' during our annual wellbeing week, and 'Online Bullying' during anti bullying week.

Managing Internet Access

Information system security

- School computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be in line with local authority guidance

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Pupils and staff must immediately tell a teacher or Online Safety Lead if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others, or confidential information about school in e-mail communication, or arrange to meet anyone without specific permission from a parent or carer.
- Staff must not reveal personal details of themselves or others, or confidential information about school in e-mail communication, websites (including social networking sites) or in chat rooms.
- Staff to pupil email communication must only take place through appropriate channels within the school setting. During school closure, this has included class email addresses. These emails must only be used during school hours and following the code of conduct staff would adhere to whilst within school. Any inappropriate or questionable emails must be immediately discussed with a member of SLT.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Communication between parents and staff will be via info@westfield.surrey.sch.uk, or using the class specific email addresses.

Remote access

- All teachers should only access emails and documents containing personal information including photographs and videos via the school remote access and shared drives.
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Head teacher and administrative assistant will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used on the website without the permission of parent/carer.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website/any other media.
- Parents should be clearly informed of the school policy on image taking and publishing. Both are available on the school website.

Social media/networking

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords in line with the school Online safety progression.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school bring a range of dangers for primary aged pupils. Information about social networks and current trends are emailed to parents and staff via our school newsletter each month.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Artificial Intelligence

As outlined in the school's Child Protection and Safeguarding Policy, Westfield Primary School recognises that Artificial Intelligence (AI) and other emerging technologies form part of the modern online landscape and therefore carry both opportunities and safeguarding risks. In line with national guidance (KCSIE 2025 and DfE AI in Education), staff and pupils must use AI tools safely, responsibly and with a clear understanding of potential risks such as inaccurate information, bias, inappropriate content, data privacy, and academic integrity.

All AI tools used in school must be risk-assessed and approved by the Digital Lead and Designated Safeguarding Lead (DSL). No personal or identifiable pupil data may be entered into any public AI system. Staff are responsible for modelling safe and critical use of AI-generated content, teaching pupils how to question reliability, and ensuring that any pupil interaction with AI happens within a supervised, age-appropriate, and educational context.

The school's AI Workforce Policy and Pupil AI Agreement set out clear expectations for safe use, and any concerns relating to misuse of AI—whether by staff, pupils, or external systems—must be reported to the DSL in line with safeguarding procedures. AI-related risks are included in the school's online safety monitoring, filtering systems, and risk register to ensure a consistent and proactive approach across all safeguarding documentation.

Pupils will be taught that AI tools can make mistakes, may contain bias, and must not be used to complete work in place of their own learning. Pupils must not use AI to generate homework, assessments or impersonate others.

Protecting professional identity

The school has a duty of care to provide a safe learning environment for pupils and staff. School staff should ensure that:

- No inappropriate reference should be made of social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school /academy or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

This policy also reflects the DfE Filtering and Monitoring Standards for Schools and Colleges.

- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Lead so that appropriate precautions can be taken and websites can be blocked for pupil access.
- The Online Safety Lead, in conjunction with school's technical support, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- The Headteacher and lead DSL (Julia Findlay) are responsible for ensuring that filtering and monitoring systems meet statutory requirements. Effectiveness is reviewed at least annually and whenever there are significant changes to technology or risk. Governors receive an annual report on filtering and monitoring.

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.
- Games machines including the Nintendo Wii, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils or parents is required. Personal phones must not be used without direct permission from the Headteacher.
- The school's online learning platform (Seesaw) allows contact between school staff and children working at home or in evenings and weekends. School staff will conduct themselves on Seesaw in the exact manner as in school. Access to each class and any contact is available via the school administrators (Karyn Hing, Kate Beatie, Fran McPhee). Each teacher accesses every class within their year group. This allows the 'open door' policy we use in school to be reflected virtually.
- When using personal devices, school emails should not be downloaded directly to the device. There should not be immediate access to school emails, through an application or mail server. If accessing school emails within the browser of a personal device, care must be taken to ensure that the account has been signed

out when finished. Two factor authentication should be used at all times. When emails are sent with attachments containing sensitive information, these should not be downloaded directly to a personal device.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the UK GDPR (2018)

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for Computing' before using any school Computing resource.
- The school will maintain a current record of all staff and pupils who are granted access to school Computing systems.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Children use child appropriate search engines in order to search for information during lessons. Whenever possible, teachers should always review sites and provide these directly to children using QR codes or hyperlinks on Seesaw.
- All children have signed a Code of Conduct before using a school resource.
- Any person working on school premises using the school network will be asked to read and adhere to a specific visitors policy before being allowed access to the Internet. Visitors to the school will be provided with a guest username and password to log on to the school network, which will allow limited access to files and programs.

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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- During Computing lessons, school staff will ensure children know that if they see something online they are not comfortable with, they are to talk to an adult. The school will encourage the view that it is not embarrassing or wrong to come across inappropriate material accidentally.

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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the Online Safety policy to pupils

- Appropriate elements of the Online Safety policy will be shared with pupils.
- Online Safety rules will be posted in all networked rooms.
- All children sign a Code of Conduct agreement at the beginning of the year.
- Before accessing any school computer, children read and agree to the Online Safety school rules.
- Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils using the Online Safety progression document.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the Online Safety policy

- All staff have access to the School Online Safety Policy via the S drive and school website and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' and carers attention will be drawn to the Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will be provided with monthly updates about Online Safety via the school newsletter.
- The school Inclusion Team and Online Safety Lead have resources available to support specific parents with any online safety concerns.
- A termly Online Safety workshop should be held virtually by school which will keep parents/carers up to date on current Online Safety issues.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Mobile Technology Guidance

- Mobile phones, E readers and SMART watches may not be brought into school by children. This is in place to safeguard the staff and children at Westfield. The exception to this is when children in Year 5 and 6 are walking to and from school independently. In this instance, their phones are passed to the class teacher at the start of the school day and retained by the office until the children are released at the end of the day.
- Staff: Mobile phones, E readers and SMART watches may not be used during lessons or formal school time. They should be switched off (or silent) at all times. The exception to this is when staff are on a school trip and need to communicate with school staff only.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

- Any device brought into school in breach of this policy will be confiscated and returned to parents/carers. Repeated breaches may result in further sanctions.
- Staff are not permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the student without specific permission from the headteacher in extreme circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to the lunch break and after school.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff should be contacted.

External Devices

- In the event that school or academy owned devices are leant to children to support learning at home, parents will be asked to sign a contract (Appendix A) on behalf of the child.

Reporting Online Safety Concerns

- Any online safety concern (content, contact, conduct or commerce) must be reported immediately to the DSL or Deputy DSL.
- Concerns will be logged on the school's safeguarding recording system.
- Where appropriate, parents/carers will be informed.
- Serious incidents may be referred to Surrey LADO, Police, CEOP or Children's Services.
- The school will preserve evidence where relevant and not view illegal content unless directed by Police.

Date: January 2026 **Date of next review: January 2027**

This policy should be read in conjunction with other relevant school policies.

APPENDIX A

PUPIL CHROMEBOOK LOAN AGREEMENT

As a parent/guardian/carer of a student to whom a Chromebook has been loaned you must sign to agree that you have read and agreed to the following terms and conditions:

- The equipment provided is the property of Westfield Primary School and is for the sole use of **XXX** in accessing home learning provision provided by Westfield Primary School.
- I understand that this equipment may be used by other family members whilst supporting my child's education but must not be used for any other activities.
- This Chromebook (complete with case & charger) must be returned to the school when my child leaves the school or when it is agreed that it is no longer required to support my child accessing home learning provision.

I agree to ensure that:

- Any user treats the equipment with appropriate care and the Chromebooks is maintained in the condition it was provided.
- The equipment is not left unattended without being stored appropriately (e.g. in your home)
- Any user avoids food and drink near the keyboard/touch pad.

I understand and agree that the school will not accept responsibility for the loss of work in the event of the Chromebook malfunctioning.

I understand and agree that it is the responsibility of my child to back-up their work regularly.

I agree to ensure that any user only uses software installed on the Chromebook when provided.

Should any faults occur, I agree that I will notify the school as soon as possible so that they may undertake any necessary repairs. Under no circumstances will I, or anyone other than school ICT staff, attempt to fix suspected hardware or software faults.

I agree and understand that the school will not accept responsibility for offering technical support relating to home internet connectivity.

I agree that any telephone and/or broadband charges incurred by any user accessing the internet from any site other than school premises are not chargeable to the school.

I will ensure that any internet access using the Chromebook at home is for an appropriate educational purpose.

I agree to ensure that appropriate filtering and monitoring is in use on the Chromebook in accordance with recommendations by my internet provider.

Parent/Guardian/Carer Signature:	
Date:	

For School Use Only

Device Name:	
Device Serial Number:	
Asset Number	
Device Issued By:	
Date:	

APPENDIX B

STAFF LOAN DEVICE AGREEMENT

Purpose
The school has purchased various devices to lend to staff members for the purpose of supporting effective working, including working from home as and when required. The device stated below has been issued to the staff member named below ("Staff Member").

Ownership of and return of devices
The issued device and any related equipment shall remain the sole property of the school and are governed by the school's policies. The device and any related equipment must be returned in their original condition to the school office immediately upon request from the school.

Personal use
The Staff Member will not use the device for any personal or commercial use and will not share the device among family or friends or loan the device or any related equipment to any other person.

Damage to, loss or theft of device
The Staff Member is responsible for the device and any related equipment at all times whether or not on the school's premises and agrees to keep the device and any related equipment in good working condition and securely stored at all time to prevent damage, loss or theft.

If the device or any related equipment becomes faulty or is damaged, lost or stolen, the Staff Member must immediately inform the School Business Manager. In the case of theft of the device or any related equipment, the Staff Member must also immediately inform the Police and provide the School Business Manager with the Police crime report reference number.

In the event of damage to or loss or theft of the device or related equipment, which is covered by the Staff Member's home contents insurance, the Staff Member will liaise with the school with regard to making a relevant claim.

If there is no clear evidence of theft or the device has been lost due to negligence by the Staff Member, the Staff Member will be fully responsible for the cost of replacing the device and any related equipment.

In the event of damage to the device or related equipment due to normal wear and tear or resulting from normal use of the device which is not the fault of the user, the school will investigate the damage and effect any necessary repairs at no cost to the Staff Member.

If there is evidence that damage to the device has been intentionally or negligently caused by the Staff Member, then the Staff Member will be fully responsible for the cost of replacing the device and any related equipment and may be subject to disciplinary action.

Acceptable use of device
The Staff Member will use the device lawfully and acknowledges that the school will monitor activity on the device.

The Staff Member has received copies of and will comply with the school's:

- ICT and Internet Acceptable Use Policy
- Data Protection Policy;
- Child Protection & Safeguarding Policy;
- Guidance Note for staff on working from home; and
- Guidance Note for staff on using video conferencing facilities.

The Staff Member agrees to comply with any instructions provided relating to password protocols and the installation of updates, antivirus and anti-spyware software as required.

The Staff Member acknowledges that if they engage in any activity that constitutes 'unacceptable use', they may face disciplinary action in line with the school's Staff Behaviour (Code of Conduct) policy.

Signature
I confirm that I have read and agree to the terms and conditions set out in this agreement and any documents referred to in this agreement.

Staff Member

Staff Member Name:	
Device Name:	
Device Serial Number:	
Staff Member Signature:	
Date:	

School

Device Issued By:	
Date:	