

Windsor Community Primary School



Online Safety Policy and Acceptable Use Policy 2025/2026

Key People

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Fiona Wright
Deputy Designated Safeguarding Leads / DSL Team Members	Jennie Karkoszka, Samantha Ginley, Ashley Douglas
Link governor for safeguarding	Sarah Murphy and Lucy Fiori
Link governor for web filtering	Paul McKenna
Curriculum leads with relevance to online safeguarding and their role	Jennie Karkoszka – PSHE and RSE Abby Smith – Computing
Network manager / other technical support	MGL
Date this policy was reviewed	October 2025
Date of next review a	September 2026

1. Purpose of this Policy

This Online Safety Policy sets out how Windsor Community Primary School will safeguard pupils, staff, and the wider school community when using digital technology and online services. It ensures compliance with:

- **Keeping Children Safe in Education (KCSIE) 2025**
- **Education Act 2011 & 2002**
- **Working Together to Safeguard Children 2024**
- **Data Protection Act 2018 / UK GDPR**
- **Online Safety Act 2023 (implemented 2025)**, including protections for children accessing online content
- **Prevent Duty**
- **Ofcom Online Safety Codes (2025)**

The policy applies to all pupils, staff, governors, volunteers, contractors, and visitors using school technology or accessing online platforms through the school.

2. Roles and Responsibilities

Governing Body

- Ensures online safety is embedded within safeguarding practice.
- Reviews this policy annually.
- Monitors risk assessments relating to online safety.

Headteacher

- Ensures policy implementation and staff training.
- Ensures systems meet statutory filtering and monitoring requirements.

Designated Safeguarding Lead (DSL) / Online Safety Lead/ Computing Lead

- Oversees online safety provision, policies, and curriculum.
- Manages online safety concerns, logs incidents, and liaises with external agencies.

- Ensures staff receive ongoing training.
- Reviews filtering/monitoring reports.

Staff

- Follow this policy and the Staff Acceptable Use Policy (AUP).
- Report concerns immediately to the DSL.
- Maintain professional conduct online.

Pupils

- Follow the Pupil Acceptable Use Policy.
- Report anything that makes them worried, uncomfortable, or unsafe.

Parents & Carers

- Support children's safe use of technology at home.
- Follow school guidance on communication and digital conduct.

3. Teaching Online Safety

Online safety is taught through:

- Computing curriculum (aligned with the National Curriculum)
- PSHE/RHE lessons
- Assemblies and themed weeks
- Cross-curricular digital literacy
- Workshops for parents

Teaching covers:

- Personal information and privacy
- Safe online behaviour & respectful communication
- Recognising harmful or inappropriate content
- Online bullying and digital citizenship
- Critical thinking, misinformation, and scams
- Safe searching
- Gaming, livestreaming, and AI-generated content
- Reporting tools (CEOP, Report Harmful Content, school systems)

4. Filtering & Monitoring

The school uses age-appropriate, highly effective filtering and monitoring systems that meet DfE and Online Safety Act 2025 expectations.

Filtering:

- Blocks illegal content (CSAM, extremism, abuse, fraud).
- Blocks adult/age-inappropriate content (pornography, gambling, violence, self-harm, controlled substances).
- Age-appropriate filtering for different key stages.

Monitoring:

- Alerts DSL to indicators of risk (bullying, grooming, self-harm, radicalisation).
- Reviewed at least termly by the DSL and Headteacher.
- Audit logs retained in line with data-protection requirements.

The school uses **Smoothwall**.

5. Use of School Devices and Networks

Pupils:

- Only use school devices under supervision.
- Use filtered internet access.
- Do not access social media unless part of a teacher-directed, curriculum-based activity.

Staff:

- Staff devices protected by passwords, encryption, and secure logins.
- No downloading unauthorised software.

- No use of personal devices to photograph or record pupils.

6. Remote Learning & Online Communication

- Only school-approved platforms may be used (e.g. Google Classroom / Microsoft 365).
- Staff must use school accounts for all pupil/parent communications.
- Video calls must use TEAMS (waiting rooms, controlled screen-sharing, recording disabled unless authorised).

7. Managing Online Safety Incidents

- All concerns reported to the DSL and logged using CPOMS.
- Incidents will follow safeguarding, behaviour, and anti-bullying procedures.
- For illegal content, the DSL will contact CEOP, LADO, police, or other agencies as required.
- Parents will be informed where appropriate.

8. Cyberbullying

The school will treat online bullying the same as face-to-face bullying.

Responses may include:

- Restorative practice
- Behaviour sanctions
- Parental meetings
- Support for affected pupils
- Reporting to external services if necessary

9. Data Protection and Privacy

- Personal data handled in line with UK GDPR.
- Staff must store and share pupil data securely.
- Pupils' digital footprints are discussed as part of the curriculum.
- The school will meet Online Safety Act 2025 expectations regarding children's data minimisation and protective design.

10. Use of AI Tools

- Staff may use AI-assisted tools only when compliant with data-protection rules.
- No pupil personal data may be uploaded to public AI tools.
- Pupils may use AI tools for learning only under supervision and with age-appropriate safeguards.

11. Social Media

Staff:

- Must not "friend" or follow pupils or parents.
- Must not post content that damages the school's reputation.
- Must not share confidential information.

Pupils:

- Taught how to use social media safely and respectfully.
- Social media access on all school devices is blocked.

Parents:

- Should not post images of other children without consent.
- Should not use social media to discuss grievances with the school.

12. Mobile Phones & Smart Devices

Pupils:

- Mobile phones are **not permitted** in school. If a child brings their phone into school it must be handed into the office, switched off and picked up at the end of the school day.

Staff:

- Personal devices must never be used for pupil photos or communication.
- Must not use their phones in front of the children

13. Acceptable Use Policies (AUPs)

The following AUPs accompany this policy and are signed annually (see appendices):

- Staff
- Pupil EYFS/KS1 & KS2 versions
- Parent/Carer
- Governor

14. Training

Staff:

- Receive annual safeguarding training including online safety (KCSIE 2025).
- Receive updates throughout the year on new risks, technologies, and legal duties.

Pupils:

- Receive continuous online safety education.

Parents:

- Offered workshops and information sessions.

15. Monitoring & Review

- The DSL monitors online safety incidents and filtering/monitoring data.
- Governors review this policy annually or following significant changes such as updates from the Online Safety Act or Ofcom.
- Risk assessments updated termly.

16. Linked Policies

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Staff Code of Conduct
- Remote Learning Policy
- Curriculum Policies

This policy will be reviewed September 2026



EYFS and Key Stage 1 Acceptable Use Policy

My name is _____

To stay **SAFE** online and on my devices, I will:

1. I only **USE** devices or apps, sites or games if I am allowed to.
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused.
3. I look out for my **FRIENDS** and tell someone if they need help.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE**.
6. Anything I do online can be shared and might stay online **FOREVER**.
7. I don't keep **SECRETS**  unless they are a nice surprise.
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must. Sometimes these can be dangerous.
9. I don't change **CLOTHES** or get undressed in front of a camera.
10. I always check before **SHARING** my personal information or other people's stories, videos and photos.
11. I am **KIND** and polite to everyone.

My trusted adults are:

_____ at school and _____ at
home



Key Stage 2 Acceptable Use Policy 2025

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my adults in school***– If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use devices, apps, sites and games if and when I am allowed to. If not sure, I will ask.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake, I don't try to hide it but ask for help.***
12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about. I check with a trusted adult before I chat with anyone for the first time, even if they are a 'chatbot'.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I check with a parent/carers before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I can say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and age restrictions. I follow rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it. I talk to others online how I would like to be spoken to.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across. I will not copy anything without permission. If I am not sure I ask a trusted adult.

~~~~~

**I have read and understood this agreement. If I have any questions, I will speak to a trusted**

**adult: at school that might be \_\_\_\_\_**

**Outside school, my trusted adults are \_\_\_\_\_**

**I know I can also get in touch with Childline or Place2Be**

**Signed: \_\_\_\_\_**

**Date: \_\_\_\_\_**





### **Staff, Governors and Volunteer Acceptable Use Policy 2025**

We ask everyone involved in the life of Windsor Community Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to read, understand, follow and sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

If you have any questions about this AUP or our approach to online safety, it is your responsibility to please speak to **Fiona Wright**

#### **What am I agreeing to?**

- I have read and understood Windsor's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
- I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
- I will report any behaviour which I believe may be inappropriate or concerning in any way (by adults or pupils) to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I identify.
- I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).
- I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.
- I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'! If I am unsure how to address any issues, I will seek support from the DSL.
- I will leave my phone in my bag and turned onto silent. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the Headteacher or Deputy Headteacher and it will be done in the presence of a member staff. The same principles apply for wearable technology. Smart glasses should not be worn in school. Please speak to Fiona Wright if this presents any issue.

- I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
- I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
- I will check with Abby Smith if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured. This includes any generative AI apps.
- I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods. [onlinesafetyprinciples.lgfl.net](https://onlinesafetyprinciples.lgfl.net)
- I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos). I will flag any concerns about “overblocking” to the DSL (such as if I cannot access teaching materials).
- I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
- I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
- During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
- I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other’s images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school’s Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
- If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
- Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.

- I will not use any new technology or download any apps without agreement from Fiona Wright or Abby Smith
- I will not use a mobile hotspot to provide internet to any device I use in school.
- I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
- I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
- I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation in relation to using these platforms.

**To be completed by the user**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:**

---

**Name:**

---

**Role:**

---

**Date:**

---



### Parent/carers Acceptable Use Policy 2025

- I understand that Windsor Community Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
- I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
- School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
- I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
- I will support my child to follow the school's policy regarding bringing devices (mobile phones, tablets, Smart watches and glasses etc.) to school. At Windsor we do not allow children to bring mobile phones, smart watches or any other recording device to school with them. If they do bring it to school they will be asked to switch it off and put it in the office until the end of the day.
- I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's advice and teaching and will not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13 years old).
- When I visit the school premises, I will keep any online technology in my pocket wherever possible.
- I will **not** share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous (see [nofilming.lgfl.net](https://nofilming.lgfl.net) for more information). The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form
- I will not covertly film or make recordings of any interactions with pupils or adults in schools. If I wish to make any recording, we request you to please speak to **Mrs Wright**
- I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to [parentsafe.lgfl.net](https://parentsafe.lgfl.net) for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
- Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks. Find out more at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
- I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
- If my child has an online tuition, I will refer to the [Online Tutors – Keeping children Safe poster](#) and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
- I understand that whilst home networks are much less secure than school ones, I can apply safety settings to my home internet and to various devices, operating systems, consoles, apps and games. Find out more at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)

- There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
- I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, role model healthy behaviours and refer to the principles of the Digital 5 A Day: [childrenscommissioner.gov.uk/our-work/digital/5-a-day/](https://childrenscommissioner.gov.uk/our-work/digital/5-a-day/)
- I will not attempt to track my child during the school day or on school trips, e.g. with Apple AirTags or similar devices. Not only is this against the terms and conditions of these products, it is unhelpful to the operation of the school, can broadcast the location of children to passing users and can lead to unnecessary distress among parents e.g. if a school trip has an unannounced change of route or schedule.
- I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen in the Online Safety Policy and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
- I can find out more about online safety at Windsor Community Primary School by reading the full Online Safety Policy and can talk to if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____