



Wrekin View Primary School and Nursery

Online Safety Policy

Date of policy creation	January 2026
Policy Lead	Mrs. F. Atherton
Frequency of review	Annually
Review due	January 2027

Contents

Wrekin View Online Safety Policy	3
1. Introduction.....	3
2. Aims.....	3
3. Scope	4
4. Roles and Responsibilities	4
4.1 The Governing Board:	4
4.2 The Headteacher:.....	4
4.3 The designated safeguarding lead (at Wrekin View this is also the headteacher).....	5
4.4 IT manager	5
4.5 All staff and volunteers	6
4.6 Parents/carers	6
4.7 Visitors and members of the community	6
5. Education and curriculum.....	6
5.1 Pupils will be taught about online safety as part of the curriculum.....	6
5.2 Pupils will be taught practical cyber security skills	7
6. Educating parents/carers about online safety	7
7. Cyber-bullying	8
7.1 Definition.....	8
7.2 Preventing and addressing cyber-bullying	8
7.3 Examining electronic devices	8
7.4 Artificial intelligence (AI)	9
8. Acceptable use of the internet in school	10
9. Personal devices	10
10. Staff using work devices outside school	10
11. How the school will respond to issues of misuse	11
12. Training for staff, governors and volunteers.....	11
13. Filtering and monitoring.....	12
14. CCTV.....	12
15. Digital images and media.....	12
16. Extremism	13
17. Data protection and cyber security	13
18. Messaging/commenting systems: authorised systems.....	13
19. Behaviour / usage principles of messaging and commenting systems	14
20. Online storage or learning platforms.....	14
21. Monitoring arrangements	14
22. Links with other policies	15

Wrekin View Online Safety Policy

1. Introduction

Online safety is an essential part of safeguarding and education in today's digital world. This policy sets out Wrekin View Primary School's approach to ensuring that all members of our school community use technology safely, responsibly, and respectfully. It explains the standards, procedures, and expectations that underpin our commitment to protecting children from online harm while enabling them to benefit from the opportunities technology offers.

This policy is written in line with Keeping Children Safe in Education (KCSIE) 2025, statutory RSHE guidance, and other relevant legislation. It is designed to complement our Child Protection and Safeguarding Policy and the Trust Central Safeguarding Framework.

This policy applies to everyone in our school community, including:

- Pupils
- All staff (teaching, support, supply, and volunteers)
- Governors
- Parents and carers
- Contractors and visitors who use school technology or engage in school-related online activity

By following this policy, we work together to create a safe, supportive, and positive online environment for all.

Key people:

Headteacher	Fiona Atherton
Designated Safeguarding Lead (DSL) – lead for filtering & monitoring	Fiona Atherton
Deputy Designated Safeguarding Leads (DDSLs)	Lesley Stephenson, Charlotte Gowen, Paul Kilburn, Hollie Taylor-Ward, Hannah Barnett, Oliver Cleevely
Curriculum leads with relevance to online safeguarding in their role	Oliver Cleevely Ross Jones
Link Governor for Safeguarding	Mollie Headley
Link Governor for Filtering & Monitoring	Mollie Headley

2. Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Wrekin View Primary School's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today and tomorrow's digital world, to survive and thrive online. Our approach to online safety is based on addressing the following categories of risk:

- › **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- › **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- › **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
 - Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - › for the protection and benefit of the children and young people in their care, and › for their own protection, minimising misplaced or malicious allegations and to better understand their › own standards and practice.
 - › for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the › reputation of the school and profession.
 - Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Behaviour Policy).

3. Scope

This policy applies to all members of the Wrekin View Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

4. Roles and Responsibilities

4.1 The Governing Board:

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

4.2 The Headteacher:

The headteacher will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The headteacher will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The headteacher will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs.

The headteacher will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The headteacher will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. They will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- › Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- › Reviewing filtering and monitoring provisions at least annually
- › Blocking harmful and inappropriate content without unreasonably impacting teaching and learning › Having effective monitoring strategies in place that meet the school's safeguarding needs

The headteacher will make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead (at Wrekin View this is also the headteacher)

- The DSL takes lead responsibility for online safety in school, in particular:
 - Reviewing this policy annually and making sure the procedures and implementation are updated and reviewed regularly
 - Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
 - Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
 - Working with the IT manager to make sure the appropriate systems and processes are in place
 - Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
 - Managing all online safety issues and incidents in line with the school's child protection and safeguarding policy
 - Responding to safeguarding concerns identified by filtering and monitoring
 - Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
 - Making sure 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 governing board
 - Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
 - Approving and denying access to websites that may be blocked due to filtering systems
- This list is not intended to be exhaustive.

4.4 IT manager

The IT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept 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 computing systems on a regular basis.

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

This list is not intended to be exhaustive.

4.5 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 making sure that pupils follow the school's terms on acceptable use.

Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting any incidents on CPOMS.

Following the correct procedures by putting a request in writing to the DSL if they need to bypass the filtering and monitoring systems for educational purposes.

Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy.

Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

4.6 Parents/carers

Parents/carers are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)
- Wake Up Wednesday provided through the National College
<https://nationalcollege.com/institutions/nationalonline-safety> - Free resources for trusted adults with information sheets provided weekly by Computing/ESafety lead through Class Dojo.
- Monthly online safety newsletter available on the school website
<https://wrekinview.lct.education/information/academy-newsletters/>

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use. Visitors and members of the community will also be expected to report any breaches of acceptable use to a DSL.

5. Education and curriculum

5.1 Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

> [Relationships education and health education](#) in primary

schools In Key Stage (KS) 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 other online technologies

Pupils in Key Stage (KS) 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

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 also invite speakers to talk to pupils about this. We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access through class specific updates, whole-school newsletters, and half-termly curriculum summaries.

5.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

6. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website, Facebook, Instagram, Class Dojo and Parent Mail. This policy will also

be shared with parents/carers. Parents will be sent a monthly E-safety newsletter and be provided updates where appropriate through the headteachers weekly newsletter.

Online safety will also be covered during parents' meetings when appropriate. Parents will be invited to a yearly update meeting regarding current online safety messages.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- > They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- > The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- > **Not** view the image

> Confiscate the device and report the incident to the headteacher immediately, who will decide what to do next. The headteacher will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#). Any searching of pupils will be carried out in line with:

- > The DfE's latest guidance on [searching, screening and confiscation](#)
- > UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Copilot and Google Gemini.

Wrekin View Primary School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Wrekin View Primary School will treat any use of AI to bully pupils very seriously, in line with our antibullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school / trust, and where existing AI tools are

used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to agree to the acceptable use of the school's IT systems and the internet. These are to be provided by the DSL at the start of the school year, signed as soon as possible and returned to the E-Safety lead. These should also form part of the school's induction process for staff. Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

9. Personal devices

Pupils from Y6 may bring mobile devices into school where they travel to and from school without a parent, but they are not permitted to use them. These devices must be handed in when pupils arrive at school so they can be securely stored throughout the school day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Our approach to pupils using mobile phones is in line with DfE, Mobile Phone Guidance. Any breach of this by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device or the pupil no longer being able to bring it into school.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they should inform the headteacher.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- > Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- > Making sure the device locks if left inactive for a period of time
- > Not sharing the device among family or friends
- > Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities. Staff must not use private mobile devices in connection to their work unless expressly granted permission to do so by the Headteacher. Examples include but are not limited to:

- ClassDojo
- Tapestry

- Time Tables Rock Stars
- Bedrock Learning

If staff have any concerns over the security of their device, they must seek advice from the IT manager.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Filtering and monitoring

DSLs ensure that Internet access and supervision is appropriate to the pupil's age. The school will apply the filtering system to all pupil technology that has internet access. Staff and pupils who discover that an unsuitable site is accessible must report this to the school's DSL. The school will report any online material it believes to be illegal to the appropriate agencies. Staff that have attempted to access a website but has been blocked can approach the DSL / Headteacher to gain access providing there is proof it is a safe website to access for staff and pupils.

The Head Teacher, IT technician and DSLs have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit pupil exposure to online risks. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, and if necessary external expertise will be drawn upon. The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential. All staff engage in regular CPD, including training through the Online National College to ensure that they are aware of updates to keeping children safe online. Staff also have access to SENSO where they can monitor all computers being used in their lessons.

We block sites which can be categorized as pornography, racial hatred, extremism, gaming, and sites of an illegal nature. If pupils discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern to the DSL and the breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child. Any material believed to be illegal will be reported immediately to the appropriate agencies, such as West Midlands Police or Child Exploitation and Online Protection command (CEOP).

We will appropriately monitor internet use on all school owned or provided internet enabled devices. If a concern is identified via monitoring approaches the DSL will be informed as appropriate. All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation. The filtering and monitoring is in line with the requirements set out in Keeping Children Safe in Education 2025.

14. CCTV

Wrekin View Primary School makes use of CCTV for the safety of the school community; therefore, photo and video images are captured in line with the UK GDPR. CCTV cameras are set up to record the outside areas of the school building, including entrances and exits.

In order to balance our community members' right to privacy and the overall safety of the school, CCTV footage is kept locally and for a limited time, as outlined in the school's CCTV policy.

Live footage can be viewed by the Headteacher and members of the office staff, whilst past footage can be accessed by the Headteacher and IT staff. Access will only be sought where necessary and in reference to safeguarding of stakeholders.

15. Digital images and media

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- for displays around the school,
- for use in paper-based school marketing,
- for online prospectus or websites,
- for social media,
- for the school communication apps,
- for a specific high-profile image for display or publication.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than their image and the school name.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Wrekin View Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils unless express permission is given by the headteacher. On these occasions, images will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

16. Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

17. Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Staff and parents are reminded regularly, at least termly and during all school events, about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

18. Messaging/commenting systems: authorised systems

Staff at this school use the email system provided by Microsoft, using the Trust domain for emails (lct.education). They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or with colleagues when relating to school/child data.

Staff at this school use Class Dojo, Tapestry, BromCom and My Child at School (MCAS) to share key information with parents/carers.

Administrative staff use school emails to communicate with parents/carers to support with the smooth running of the school.

The systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

The use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be reported to the DSL (if by a child) or to the Headteacher (if by a staff member).

19. Behaviour / usage principles of messaging and commenting systems

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

- Data protection principles will be followed at all times when it comes to all school communications, in line with the trust Data Protection Policy and only using the authorised systems mentioned above.
- Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).
- Under no circumstances should school email accounts be used for personal reasons. Doing so may result in disciplinary action.

20. Online storage or learning platforms

The school uses a range of secure, educational platforms to support teaching, learning, assessment and communication. These include Microsoft One Drive, Tapestry for Early Years, Insight Tracking for pupil data, BromCom as the school's Management Information System (MIS), and online learning tools such as Bedrock Learning and Times Tables Rock Stars (TTRS).

Access is granted according to user role to ensure appropriate permissions and accountability. All platforms used by the school are GDPR compliant and meet the requirements of the Data Protection Act 2018. Only data necessary for educational and administrative purposes is shared, and access remains restricted to members of the school community. Platform settings and permissions are reviewed annually to ensure continued compliance and data security.

Parental engagement is encouraged through the Tapestry platform, where parents can view and contribute to their child's online learning journal.

Through the careful selection, management and monitoring of these platforms, the school ensures that pupils can safely benefit from high-quality digital learning experiences within a secure and well-governed online environment. All online platforms operate under the school's wider filtering and monitoring arrangements to ensure safeguarding oversight at all times. Any new platforms will be approved by the headteacher.

21. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

22. Links with other policies

This online safety policy is linked to our:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff code of conduct
- › Data protection policy and privacy notices
- › Complaints procedure
- › ICT and internet acceptable use policy