Willow Tree Academy

Online Safety Policy incl. monitoring and filtering

Date Published	September 2025
Version	3
Last Approved Date	
Review Cycle	Annually
Review Date	September 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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, fake news, 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 them 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board 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 governing board 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 governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE 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 their safeguarding needs.

The governor who oversees online safety is Tony Trueman
All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure 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

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure 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
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT 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 policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT 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 ensure 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 ICT 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 ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 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 ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 Willow Tree Academy.
- Following the correct procedures by contacting IT Services if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet. Pupil personal device policy.

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
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

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
- Relationships and sex education and health education in secondary 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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. 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. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

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.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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.
More information is set out in the acceptable use agreements in appendices 1 to 3.

8. 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.
Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from Head Teacher.

9. 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 policies on acceptable usage, Pupil personal device. 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 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.

11. Training

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 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.

12. Pupil Filtering & Monitoring: Netsweeper OnGuard+

This school is committed to providing a safe online environment for all pupils and staff, in line with our statutory duties under "Keeping Children Safe in Education" (KCSIE) and the Department for Education's Filtering and Monitoring Standards. To achieve this, we utilise **Netsweeper OnGuard+** as our primary web filtering and digital safeguarding solution.

12.1 Purpose of Filtering and Monitoring

The purpose of implementing Netsweeper OnGuard+ is to:

- **Prevent Access to Harmful Content:** Block access to illegal, inappropriate, and harmful online material, including but not limited to, content related to child sexual abuse, terrorism, self-harm, violence, hate speech, and illegal substances.
- **Identify and Respond to Safeguarding Concerns:** Proactively monitor online activity to identify potential safeguarding risks, such as cyberbullying, radicalisation, grooming, or signs of mental health distress (e.g., self-harm or suicidal ideation).
- **Support Digital Literacy and Responsible Use:** While providing a safe environment, we also aim to support pupils in developing their own critical thinking and understanding of online risks, as outlined in our curriculum.
- **Meet Statutory Requirements:** Ensure the school fully complies with its legal obligations regarding online safety and safeguarding.

12.2 How Netsweeper OnGuard+ Works

Netsweeper OnGuard+ is an AI-detected, human-verified digital safeguarding solution that integrates seamlessly with our existing web filtering. Its key functionalities include:

- **Real-time Content Filtering:**
    - Our filtering system dynamically categorises and blocks access to websites and online content based on predefined categories, keywords, and URLs.
    - It incorporates essential blocklists from the Internet Watch Foundation (IWF) and the Counter-Terrorism Internet Referral Unit (CTIRU) to prevent access to illegal content.
    - Filtering is applied to all school-managed devices, devices using the school's internet connection (including personal devices under our BYOD scheme, where applicable), and guest accounts, both on-site and when devices are taken off-site.

    - Filtering profiles are tailored to different user groups (e.g., pupils, staff) to ensure age and role-appropriate access to online content.
    - The system aims to prevent circumvention techniques (e.g., VPNs, proxies) where possible and alerts staff to such attempts.
- **Proactive Digital Safeguarding and Monitoring (Netsweeper OnGuard+):**
    - OnGuard+ monitors user activity on all supported school devices, both online and offline. This includes scanning visible content on web pages, documents, and messages, and capturing screenshots using Optical Character Recognition (OCR) technology where potential risks are identified.
    - Advanced AI technology detects and flags potential risks to student safety and well-being, automatically assigning categories and priorities to each captured event.
    - A crucial element of OnGuard+ is the **human-verified review** process. Alerts generated by the system, particularly high-priority ones, are reviewed by a team of trained Netsweeper safeGuard Specialists. This human oversight helps to contextualise alerts, reduce false positives, and ensure accurate identification of genuine safeguarding concerns.
    - The system provides real-time alerts to designated school personnel, primarily the Designated Safeguarding Lead (DSL) and relevant IT staff, allowing for prompt intervention when a potential threat arises.
    - Intuitive dashboards provide visual overviews and trend analytics, enabling our safeguarding team to monitor activity and identify patterns or changes in behaviour over time.
    - All identified incidents are recorded and tracked within the OnGuard+ system to support effective case management and follow-up.

12.3 Roles and Responsibilities

- **Governing Body** Has overall strategic responsibility for ensuring appropriate filtering and monitoring systems are in place and regularly reviewed, receiving assurance that standards are being met.
- **Designated Safeguarding Lead (DSL)** Holds lead responsibility for responding to safeguarding concerns identified by Netsweeper OnGuard+, prioritising alerts, managing incidents in line with the school's Child Protection and Safeguarding Policy, and providing reports to the governing body.
- **IT Lead/Network Manager** Responsible for the day-to-day management, configuration, and technical effectiveness of the Netsweeper OnGuard+ system, ensuring it is operational, up-to-date, and applied across all relevant devices and networks. They will also manage user profiles and respond to technical issues.
- **All Staff** Are aware that online activity is monitored and understand how to report any concerns, whether identified through OnGuard+ alerts or personal observation, to the DSL immediately.

12.4 Review and Effectiveness

The effectiveness of our Netsweeper OnGuard+ filtering and monitoring provision will be reviewed at least annually by the DSL, IT Lead, and members of the Senior Leadership Team, and reported to the Governing Body. This review will consider:

- The continued alignment with DfE Filtering and Monitoring Standards and KCSIE.
- The effectiveness in blocking harmful content and identifying safeguarding risks.
- Any necessary adjustments to filtering categories, monitoring thresholds, or user profiles.
- The impact on teaching and learning.
- Feedback from staff and pupils.
- Changes in technology use or identified safeguarding risks (e.g., new online trends).

12.5 Data Protection and Privacy

The school recognises the importance of data protection and privacy in relation to online monitoring. All monitoring carried out through Netsweeper OnGuard+ will be conducted in a manner compliant with UK GDPR and the Data Protection Act 2018. Pupils and staff are informed that their online activity on school systems is monitored, as outlined in this policy and our Acceptable Use Policies. Data retained by Netsweeper OnGuard+ is used solely for safeguarding purposes and managed according to our Data Retention Policy.

13 Staff Device Monitoring

The school provides technology resources, including devices and network access, to staff to facilitate their professional duties and enhance teaching and learning. To ensure the safety of our school community, the security of our data, and to uphold professional standards, staff device use is subject to monitoring. This is undertaken in compliance with all relevant legislation, including the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018, and is proportionate to the risks identified.

13.1 Scope of Staff Device Monitoring

Monitoring applies to:

- **All school-provided devices:** Laptops, tablets, mobile phones, and any other devices issued by the school for professional use, whether used on or off the school premises.
- **Any device connected to the school's network:** This includes personal devices (BYOD - Bring Your Own Device) used by staff to access the school's Wi-Fi or wired network.

13.2 Purpose of Staff Device Monitoring

Monitoring of staff device usage serves the following purposes:

- **Safeguarding Children:** To identify and address any activity that could pose a safeguarding risk to children, including access to or creation of inappropriate content, or communications that raise concerns about a staff member's conduct with children.
- **Data Security and Confidentiality:** To protect the school's sensitive data, including pupil and staff personal information, from unauthorised access, use, or disclosure.

- **Maintaining Professional Conduct:** To ensure that staff use school resources and technology in a manner consistent with the school's Staff Code of Conduct, IT Acceptable Use Policy, and professional standards.
- **Network Security and System Integrity:** To detect and prevent malicious activity (e.g., malware, phishing attempts) that could compromise the school's IT infrastructure.
- **Compliance with Legal and Regulatory Obligations:** To meet our statutory duties regarding online safety and other relevant legal frameworks.
- **Resource Optimisation:** To ensure school resources are used efficiently for legitimate educational and administrative purposes.

13.3 How Staff Device Monitoring is Conducted (Netsweeper OnGuard+ and other systems)

In addition to the filtering capabilities of Netsweeper nFilter applied to staff devices, Netsweeper OnGuard+ (where deployed on staff devices) and other IT systems will be used for monitoring, which may include:

- **Web Filtering Logs:** Records of websites visited, categories accessed, and any blocked attempts.
- **Activity Monitoring (Netsweeper OnGuard+):** Where OnGuard+ is deployed on staff devices, it may monitor and log visible content on web pages and applications, and capture screenshots if specific keywords or suspicious activities related to safeguarding risks are detected.
- **Network Logs:** Records of network traffic, bandwidth usage, and connections made.
- **Email and Messaging Logs:** Records of internal and external communications, including sender, recipient, subject, and in specific circumstances (e.g., safeguarding investigation), content.
- **File Access and Transfer Logs:** Records of files accessed, created, modified, or transferred on school systems or cloud storage.
- **Application Usage Logs:** Records of applications launched and time spent using them.
- **System Audit Logs:** Records of administrative actions and system changes.

Monitoring is typically automated and alert-based, focusing on identifying deviations from acceptable use or potential safeguarding/security risks. Direct, proactive human review of individual staff member's general activity is not routinely performed but may occur if an alert is triggered or as part of a formal investigation.

13.4 Transparency and Notification

All staff are informed that their use of school-provided devices and the school's network is monitored. This policy serves as formal notification of our monitoring practices. Staff are also required to sign an Acceptable Use Policy (AUP) which outlines expected behaviour and the school's approach to monitoring.

13.5 Data Handling and Confidentiality

- All data collected through monitoring systems is treated as confidential and is handled in accordance with the school's Data Protection Policy.
- Access to monitoring data is strictly limited to authorised personnel (e.g., DSL, IT Lead, Senior Leadership, HR) on a need-to-know basis for legitimate purposes (e.g., safeguarding investigation, security incident response).
- Data is retained only for as long as necessary to fulfil the purposes for which it was collected, in line with the school's Data Retention Schedule.
- Any data gathered through monitoring that indicates a potential safeguarding concern will be handled in accordance with the school's Child Protection and Safeguarding Policy. Where data indicates a potential breach of the Staff Code of Conduct or other school policies, it will be handled in line with HR procedures.

13.6 Justification and Proportionality

The school's monitoring practices are regularly reviewed to ensure they remain justified, proportionate, and necessary for the stated purposes. We balance the need for security and safeguarding with the legitimate privacy expectations of our staff. Less intrusive methods are considered where they are equally effective in achieving the desired outcome.

13.7 Staff Concerns

Any staff member who has concerns about the school's monitoring practices or wishes to clarify aspects of this policy should speak to the Headteacher or their line manager in the first instance. Further information regarding data protection rights can be obtained from the school's Data Protection Officer (DPO).

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Pupil Personal Device Policy.