



E-Safety/Acceptable Use Policy

2026- 2027

Document Type:	Colleague Responsible:	Date:	Next Review:
School	VRO	September 2026	September 2027
Approved By Finance, Audit, Risk and Health and Safety Committee			

Equality Statement

Wrotham School promotes equality of opportunity. We are committed to take a positive stand to ensure all stakeholders have a right to equality of opportunity and achievement regardless of race and ethnicity, faith, belief and religion, disability and access, age, gender identification, sexual orientation, and marital status.

Equality of opportunity is related to all areas of the schools work and is a fundamental aspect of the ethos of the school.

Introduction

Wrotham School believes that the use of information and communication technologies in Schools brings great benefits when used safely and productively.

This e-Safety Policy is part of wider Safeguarding Policies and should be read alongside the following:

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- CCTV Policy
- CET Communications Policy
- Data, Privacy and GDPR Policy
- Exam Policies
- FOI Policy
- Mobile Phone and Social Media Policy
- Safer Recruitment Policy
- Curriculum Policy
- AI Policy – AI Malpractice Policy
- Filtering and Monitoring Policy

The E-Safety/Acceptable Use Policy and its implementation will be reviewed annually.

This policy complies with Keeping Children Safe in Education (KCSIE) 2026 and reflects our obligations under the Data Protection Act 2018, UK GDPR, and the Data (Use and Access) Act 2025.

KEY STAFF

DSL: Laura Abbott

DDSL: Victoria Ross, Allison Sanders, Katy Renshaw, Ben McCracken, Amber Parris

School e-Safety Coordinator: Paul Kitney (Network Manager)

E-Safety/Safeguarding Governor: Maria Watson

Trust Safeguarding Lead: Michael Cater

Statement of Aims:

At Wrotham School we aim to offer an IT and online network that is beneficial to students, parents, staff and visitors in learning, experiencing and staying safe and secure. The use of IT in School, when learning and in its extended communications with stakeholders, aims to improve and move forward the work we do as an educational institution underpinning our high expectations of everyone involved.

This policy is both a set of clear expectations, a guide for the School community and a source of information to improve e-Safety at the School and in wider experiences.

The following is a list of online locations linked directly to the School. Information and resources on these sites are produced, monitored and controlled by the School:

www.wrothamschool.com

School Website

<https://wrothamschoolsixthform.wordpress.com>

Sixth Form Website

<https://www.wrothamschool.com/careers/careers-at-wrotham-school/> **Careers Website**

<http://charactereducationtrust.org.uk/>

MAT Website

<https://www.whatsapp.com/channel/0029VaEDz2a47Xe6xLoas23F>

WHATSAPP

Filtering and Monitoring

Our Commitment

Wrotham School is committed to doing all it reasonably can to limit children's exposure to online safety risks through appropriate filtering and monitoring systems. Keeping Children Safe in Education (KCSIE): summary (The Key Leaders)

Responsibilities

The Governing Body will:

- Ensure our child protection and online safety policies cover appropriate filtering and monitoring on school devices and school networks
- Review the effectiveness of our filtering and monitoring systems at least once every academic year
- Ensure the leadership team and relevant staff understand the provision in place and can manage it effectively
- Consider the age range of pupils, those potentially at greater risk of harm, and how often they access IT systems when reviewing our approach

The Senior Leadership Team member responsible for filtering and monitoring (supported by the DSL and Network Manager) will:

- Conduct an annual review of our filtering and monitoring systems
- Review the DfE's filtering and monitoring standards and discuss with IT staff what needs to be done to meet these standards
- Document the review process and any actions taken
- Ensure filtering and monitoring requirements apply to generative AI tools and platforms

Our Network Manager (Paul Kitney) will:

- Implement and maintain appropriate filtering and monitoring systems
- Support the annual review process
- Escalate any concerns identified through monitoring to the DSL immediately
- Ensure systems are balanced to avoid 'over-blocking' that could unreasonably restrict educational content

Our Approach

- We maintain filtering systems that are appropriate for our pupils' age range (11-16)
- We monitor internet usage on school devices and networks to identify safeguarding concerns
- We consider the number of pupils, their ages, and those potentially at greater risk when determining appropriate levels of filtering and monitoring
- We ensure our approach includes oversight of generative AI tools and platforms
- We balance safeguarding with ensuring pupils can access appropriate educational content

Privacy and Monitoring

All users should be aware that:

- The school monitors and records all use of its ICT resources, including internet access, email, and use of AI tools
- Users should have no expectation of privacy when using school ICT resources
- This monitoring applies to students, staff, and visitors
- Monitoring is conducted to ensure compliance with this policy and to safeguard children

Annual Review

We will conduct a formal review of our filtering and monitoring systems at least once every academic year. This review will:

- Assess whether current systems are effective in limiting exposure to online risks
- Consider any incidents or near-misses that have occurred
- Review whether systems are proportionate and avoid over-blocking
- Assess compliance with DfE filtering and monitoring standards
- Consider emerging risks, including those related to AI
- Document findings and any actions required

To ensure this policy is clear and easy to reference, we have divided it into key aspects of e- Safety and described our objectives and expectations in regard to each element:

Acceptable Use Policy

All students, parents and staff have an implicit responsibility to keep a broad and general knowledge of how to safely and legally use computer and online technology. Ignorance of technology is never an excuse for behaviour which may cause harm someone else.

Much of the principles of this document are common sense and should be considered as such. Behaviours online or when using technology should not differ to society and the laws expectations of behaviour and responsibility.

We all have a responsibility to safeguard children: this includes online.

Introduction

This Acceptable Use Policy (AUP) outlines the expectations and responsibilities of students, staff, and visitors at Wrotham School regarding the use of Information and Communication Technology (ICT) resources. This includes all hardware, software, network services, and internet access provided by the school.

Purpose

The purpose of this policy is to ensure that ICT resources are used in a safe, respectful, and appropriate manner that supports the educational and administrative goals of the school.

Scope

This policy applies to all users of the school's ICT resources, including students, staff, and visitors, regardless of whether the use occurs on or off school premises.

General Principles

1. **Responsible Use:** All users must use ICT resources responsibly, ethically, and lawfully.
2. **Educational Purpose:** ICT resources are provided primarily for educational purposes and school-related activities.
3. **Respect for Others:** Users must respect the privacy, rights, and feelings of others at all times.
4. **Safety and Security:** Users must take reasonable precautions to ensure their own safety and the security of the school's ICT resources.

Acceptable Use

1. Students:

- Access the internet and school network for educational purposes.
- Follow teachers' instructions regarding the use of ICT in lessons.
- Respect the privacy and work of others by not accessing or interfering with their files or accounts.
- Report any inappropriate material or misuse of ICT resources to a teacher or staff member immediately.

2. Staff:

- Use ICT resources to support teaching, learning, and administrative tasks.
- Model responsible use of ICT for students.
- Protect sensitive and confidential information by following data protection guidelines.
- Monitor and guide student use of ICT to ensure compliance with this policy.

3. Visitors:

- Use ICT resources only with permission from school staff.
- Follow all relevant school policies and guidelines when using ICT resources.

Unacceptable Use

1. General Prohibitions:

- Accessing, creating, or distributing material that is illegal, offensive, inappropriate, or in breach of the responsibility to safeguard students and staff
- Using ICT resources for personal financial gain, gambling, or political purposes
- Engaging in cyberbullying, harassment, or any form of disrespectful communication including on social media
- Engaging in or promoting misogyny or misandry through online communications or content
- Attempting to bypass network security or access restricted areas of the school network
- Using AI or unreferenced/copied internet resources and presenting this as "own work" in assessed or submitted work
- **Making or sharing nudes or semi-nudes (images or videos), including:**
 - Images or videos that are wholly or partially created, altered, or manipulated using artificial intelligence (AI), including deepfakes
 - Any image or video of a sexual nature involving children under 18
 - Sharing such content, even if created or shared with apparent consent
- **Any incident involving the making or sharing of nudes or semi-nudes will be treated as a safeguarding matter and reported to the DSL immediately**

2. Network and System Integrity:

- Installing or using unauthorized software or hardware on school ICT resources
- Intentionally damaging, disabling, or disrupting ICT equipment or services
- Sharing passwords or using another person's login credentials
- Using the school Wi-Fi or network system to access any sites, activity, or inappropriate content including behaving in an inappropriate or unlawful way, as per this policy
- Using generative AI tools in ways that:
 - Breach copyright or intellectual property rights
 - Create harmful, offensive, or inappropriate content
 - Attempt to circumvent safeguarding measures
 - Violate data protection principles

3. Exploitation and Harm:

The school recognizes that children can be at risk of various forms of exploitation online, including:

- **Criminal exploitation** – being coerced into criminal activity, including county lines drug trafficking
- **Sexual exploitation** – being manipulated or coerced into sexual activity or sharing sexual images
- **Financial exploitation** – being manipulated into providing money, financial information, or engaging in fraudulent activity
- **Modern slavery** – being recruited, controlled, or exploited through online platforms

Any concerns about these forms of exploitation must be reported to the DSL immediately.

Monitoring and Privacy

- The school reserves the right to monitor and record all use of its ICT resources to ensure compliance with this policy.
- Users should have no expectation of privacy when using school ICT resources, including email and internet access. This is the same for staff, students and visitors.

Consequences of Misuse

- **Students:** Misuse of ICT resources may result in disciplinary action in accordance with the school's behaviour policy. This may include loss of ICT privileges, detention, or more severe sanctions.
- **Staff:** Misuse of ICT resources may result in disciplinary action in accordance with employment policies. This could include formal warnings, suspension, or termination of employment.
- **Visitors:** Misuse of ICT resources may result in the withdrawal of access privileges and could lead to being barred from school premises.

When unlawful activity has taken place – the school will report this to the police, social services, LADO or other relevant body as appropriate.

Reporting Issues

- Users are encouraged to report any concerns or incidents related to ICT use to a teacher, IT staff, or school administration promptly.
- Where there is a safeguarding risk this should be reported to the DSL (Mrs L Abbott/ Miss V Ross/ Mrs A Sanders) without delay.

AI and Online Safety

Artificial Intelligence (AI) and Generative AI

Safeguarding Considerations

The school recognizes that AI technologies, particularly generative AI, present both opportunities and risks for safeguarding.

Staff Responsibilities

All staff must be aware that:

- AI tools can be used to create, alter, or manipulate images and videos of children (deepfakes)
- Any incident involving AI-generated or AI-altered nudes or semi-nudes of children is a safeguarding matter requiring immediate reporting to the DSL
- Children may not understand the risks of using AI tools or sharing personal information with AI platforms
- AI tools may be used to facilitate bullying, harassment, or exploitation

Acceptable Use of AI

Students may use AI tools for educational purposes when:

- Explicitly permitted by teaching staff for a specific task
- Used transparently – students must declare when AI has been used in their work
- Used appropriately – following school guidelines and teacher instructions
- Supervised – under appropriate adult oversight

Students must not use AI tools to:

- Create, alter, or share images or videos of other people without explicit permission
- Generate inappropriate, harmful, or offensive content
- Circumvent assessment requirements or present AI-generated work as their own
- Bypass filtering or monitoring systems
- Access age-inappropriate AI platforms or services

Data Protection and Privacy

When using AI tools, all users must:

- Not input personal data about themselves or others into AI systems without permission
- Understand that data shared with AI tools may be stored, processed, or used by third parties
- Follow school guidance on which AI platforms are approved for use
- Be aware that the school's filtering and monitoring systems include oversight of AI tool usage

Reporting Concerns

Any concerns about AI-related safeguarding issues, including deepfakes, inappropriate content generation, or misuse of AI tools, must be reported immediately to:

- The DSL (Mrs L Abbott / Miss V Ross/ Mrs A Sanders) for safeguarding concerns
- The Network Manager (Paul Kitney) for technical or access concerns
- Any member of staff, who will escalate appropriately

Further guidance on the educational use of AI can be found in our separate AI Policy and AI Malpractice Policy.

Safeguarding Vulnerable Groups Online

The school recognizes that some groups of children may be at potentially greater risk of harm online and require additional consideration and support. Any concerns must be reported to the DSL immediately.

Young Carers

- Caring responsibilities can impact pupils' attendance, attainment, behaviour, and wellbeing
- Young carers may rely more heavily on online connections and support
- Staff should be alert to young carers who may be isolated or targeted online
- The DSL will work with relevant services to ensure young carers receive appropriate support

Children with Medical Conditions

- We will make a safeguarding referral if we have concerns that a young person might be at increased risk of being neglected, abused, or exploited online because of their medical condition
- This includes situations where access to online services is essential for a child's wellbeing but may also present risks
- Staff should consider how medical conditions might make children more vulnerable to online exploitation

Children with Special Educational Needs (SEN) and/or Disabilities

- Additional barriers can exist to recognizing abuse, neglect, and exploitation in children with SEN and/or disabilities
- These children may be disproportionately affected by online bullying
- Communication barriers may make it difficult for these children to report online abuse
- Staff should ensure online safety education is adapted for children with SEN and/or disabilities
- The school will ensure appropriate support is in place for these children to use technology safely

Children Who Need a Social Worker

- Children who need a social worker due to abuse, neglect, exploitation, and/or complex family circumstances may be particularly vulnerable online
- The DSL will hold information about which children have a social worker and use this to inform decisions about online safety support
- Staff should be particularly alert to online risks for these children

Children at Risk of Exploitation

Staff should be particularly vigilant for signs that children may be at risk of:

- **Criminal exploitation** – including through online recruitment for county lines or other criminal activity
- **Sexual exploitation** – including through online grooming or coercion
- **Financial exploitation** – including through online scams, gaming, or manipulation
- **Modern slavery** – including online recruitment or control

Additional Information:

For Students and Parents

Mobile Phones and Devices

Wrotham School operates as a mobile phone-restricted environment to support learning and safeguarding. Detailed information about mobile phone and social media use is available in our Mobile Phone and Social Media Policy: [Mobile Phone and Device Policy.docx](#)

Curriculum and Education

- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use
- Education will include understanding of online exploitation risks, including criminal, sexual, and financial exploitation
- Students will learn about the risks of AI tools, including deepfakes and inappropriate content generation
- Teaching will cover the making and sharing of nudes or semi-nudes, including AI-generated images, and why this is never acceptable

Detailed information about the curriculum can be found here:
<https://www.wrothamschool.com/information/our-curriculum/>

Copyright, Assessment, and AI

- The school will ensure that the copying and subsequent use of internet-derived materials by pupils complies with copyright law and exam and assessment regulations
- This regulation includes the use of AI
- The school will check for undeclared use of AI when suspected, in line with all published exam board rules and regulations
- Students must declare when they have used AI tools in their work

Internet Access and Filtering

- Internet and online access levels will be reviewed to reflect curriculum requirements and the age of pupils
- The school operates filtering and monitoring systems to protect students from harmful content
- These systems include oversight of AI platforms and tools

Agreement to Code of Conduct

When joining the school, students and parents will automatically be assumed to agree with this school-based code of conduct that ensures safety and security through active and responsible use of the internet.

Reporting Concerns

- Online bullying can be reported via the "report bullying" link on the front page of our school website, or in person to any member of staff
- All staff are trained to pass concerns on to be managed promptly
- **Any concerns about the making or sharing of nudes or semi-nudes (including AI-generated images) must be reported immediately**

Communications

We expect all communications with the school to follow our Communications Policy, which can be found here: <https://www.wrothamschool.com/statutory-documents-policies/>

We Will Not Tolerate or Accept:

- Bullying or intimidating others online using phones, social networking sites, and apps
- Racist, sexist, transphobic, homophobic, or other discriminatory messages, statuses, or comments made online in any context
- Misogynistic or misandrist content or communications
- The publishing of anything online that may unfairly bring the school into disrepute
- Public discussion about school matters or incidents online that involve others
- Any behaviour online that is considered slanderous, illegal, or would not be accepted in school
- **The making or sharing of nudes or semi-nudes, including AI-generated or AI-altered images**

Advice for Parents:

Social Media:

- The school strongly advises against students, particularly under-16s, using and being given access to social media
- Most social media platforms have a minimum age requirement of 13, and some require users to be 16 or older

Online Safety:

- The internet and social media pose significant and real dangers to children's safety
- Encourage your child to share and be open about their online behaviour with you – this supports their safety
- The school encourages parents to take a "when it happens to my child" approach to online safety, rather than "if it happens"
- Be aware of new risks, including AI-generated content and deepfakes

Friendships and Contacts:

- Students should not befriend anyone online they do not know or are not friends with in real life
- We often find students are "online friends" with the same people who are bullying them
- Students should block anyone who they feel is being abusive

Legal Responsibilities:

- The same rules that apply in society and by law apply to online behaviour
- Students who break these laws risk prosecution, including for:
 - Online harassment
 - Hate speech
 - Racism and homophobia
 - Making or sharing nudes or semi-nudes (even if consensual)
 - Creating or sharing AI-generated harmful content
- Please openly discuss the seriousness of consequences for this behaviour with your child

Practical Safety Measures:

- Students should not engage with online bullying or abuse of others
- Be aware of duplicate or extra devices such as second phones, online games consoles, and smart TVs which can access the same online content even after confiscating a mobile phone
- Internet access and access to mobile phones should be removed overnight to prevent disturbance to sleep and unhealthy, unmonitored access
- Monitor your child's use of AI tools and platforms

School Communication:

- The school will inform parents/carers of any incidents or concerns as and when required
- Parents' attention will be drawn to updates to the school e-Safety strategy in newsletters and on the school website
- Parents will be requested to sign an e-Safety/Internet Agreement as part of the Home School Agreement

More information on keeping your child safe online can be found here:

<https://www.wrothamschool.com/staying-safe-online/>

FOR STAFF

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct:

System Use and Security

- I understand that school information systems may not be used for private purposes
- I understand that my school information systems, internet, email, and use of AI tools will be monitored and recorded to ensure policy compliance
- I will respect system security and will not disclose any password or security information to anyone other than an authorized system manager
- I will not share the use of my IT devices with others, including family
- I will not install any software or hardware without permission
- I will not attempt to bypass filtering or monitoring systems

Data Protection and Privacy

- I understand my obligations under the Data Protection Act 2018, UK GDPR, and the Data (Use and Access) Act 2025
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises, or accessed remotely
- I will not input personal data about students or colleagues into AI systems without appropriate authorization
- I will respect copyright and intellectual property rights

Safeguarding Responsibilities

- I have read Part One of Keeping Children Safe in Education (KCSIE) in full and understand my safeguarding responsibilities
- I will report any incidents of concern regarding children's safety to the DSL/DDSL/Headteacher immediately, including:
 - Concerns about online exploitation (criminal, sexual, financial, or modern slavery)
 - Any incidents involving the making or sharing of nudes or semi-nudes, including AI-generated images
 - Concerns about harmful sexual behaviour (HSB)
 - Evidence of misogyny or misandry
- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use, communications, and publishing
- I understand that I must maintain an attitude of professional curiosity and "it could happen here" regarding safeguarding concerns

Professional Conduct Online

- I will ensure the content I publicly publish online, including posts and content written or endorsed by me on social networking sites such as Twitter and Facebook, in no way brings myself as a professional, the school, or the teaching profession into disrepute
- I will ensure that I take all steps to make personal data and online profiles private and secure
- Staff must not link, friend, follow, or add pupils currently at Wrotham School or former students under the age of 18
- Staff should be aware that their online activity may be seen by students who have mutual friends or links (this also applies to other social networking sites)
- I will ensure that my behaviour online reflects the equivalent published behaviours expected by the current professional guidelines that relate to teachers' conduct

Artificial Intelligence (AI)

- I will use AI tools responsibly and in accordance with school policy
- I will not use AI to create inappropriate content or to circumvent safeguarding measures
- I will model appropriate use of AI for students

- I will be vigilant for misuse of AI by students, including the creation of deepfakes or inappropriate content
- I understand that concerns about AI-generated images of children are safeguarding matters

Understanding and Responsibility

- It is the responsibility of individual staff members to understand how independent online services such as Facebook or Twitter work
- If an individual does not fully understand how to manage their privacy or online footprint, the school recommends they avoid using these services
- I understand my role in the school's filtering and monitoring systems and will escalate concerns appropriately

Staff are required to sign an acceptable use IT code of conduct as required/updated and when employed by the school.

The Network/ Ownership

- The school retains the right of ownership of documents or resources created by staff whilst in the paid employment of the school.
- Staff must not remove or copy/ share school resources without the express permission of the Head teacher.
- The school has the right to freeze/ monitor or withhold access to school-based accounts of staff and students at any time.

If you have any concerns about safety or behaviour online please contact safeguarding@wrotham.kent.sch.uk