



Walthamstow School For Girls

"Neglect not the gift that is in thee"

Policy Document

Online Safety Policy

Author(s):	Dave Shackson
Ratification Date:	December 2025
Next Review Date:	Autumn 2026
Reference:	OS_POLICY_VI.0

1	Aims	3
2	Legislation and guidance	3
3	Roles and responsibilities	3
4	Educating students about online safety	6
5	Educating parents/carers about online safety	6
6	Cyber bullying	7
7	Acceptable use of the internet in school	8
8	Students using mobile devices in school	9
9	Staff using work devices outside school	9
10	How the school will respond to issues of misuse	9
11	Training	9
12	Monitoring arrangements	10
13	Links with other policies	10
	Appendix A	11
	Appendix B	12
	Appendix C	13

I. AIMS

Our school aims to:

- have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- identify and support groups of students 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.
- **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 students’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study

3. ROLES AND RESPONSIBILITIES

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will make sure all staff undergo online safety training as part of Child Protection and Safeguarding training, and ensure staff understand the expectations and their roles and responsibilities around filtering and monitoring.

The Governing Body 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 Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and to monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body 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 Governing Body 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 those 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 & Learning
- having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- ensure they have read and understood this policy
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix C)
- ensure that online safety is a running and interrelated theme while devising and implementing their whole-school 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 students 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

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our child protection and safeguarding policy, including their 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 Body 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 Network Manager to make sure the appropriate systems and processes are in place
- working with the Headteacher, Network 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 Safeguarding Policy
- ensuring that any online safety incidents are logged (see Section 12) 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's Behaviour Policy
- updating and delivering staff training on online safety (Appendix C contains a self-audit for staff of 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 Body
- 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 the relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network 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 students 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 monthly 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 (see section 12) 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's Behaviour Policy
- liaise with the SLT member with ICT oversight on issues that arise pertaining to online safety.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors, 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 B) and ensuring that students follow the school's Acceptable Use Agreement (Appendix A)
- 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 informing a member of the safeguarding team and making an entry in the Safeguard logging programme.
- following the correct procedures by informing the Network Manager 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 (see section 12) 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's 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 (Appendix A)
- 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 International](#)
 - parent/carer resource sheet – [Childnet International](#)

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 be expected to read and follow it. If appropriate, they will be expected to agree to the school's Acceptable Use Agreement (Appendix B).

4. EDUCATING STUDENTS ABOUT ONLINE SAFETY

Students will be taught about online safety as part of the curriculum:

In **KS3** students will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **KS4** will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- how to report a range of concerns

By the **end of secondary school**, students will know:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- what to do and where to get support to report material or manage issues online
- the impact of viewing harmful content
- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including prison
- how information and data is generated, collected, shared and used online
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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 students with SEND.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The school will raise parent/carer 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.

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 one person or group by another person or group, where the relationship involves an imbalance of power (see also the school's Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

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

In PSHE lessons, the school will actively discuss cyber-bullying with students, 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 students, as part of Safeguarding training (see section 11 for more detail).

The school also includes information on cyber-bullying on its website, including a CEOPs link so that parents/carers 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's Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, 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 the material is illegal. They will also work with external agencies if it is deemed necessary to do so.

6.3 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 students
- is identified in the school rules as a banned item for which a search can be carried out
- 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 students and staff. If the search is not urgent, they will seek advice from DSL
- explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- seek the student'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 'good reason' to do so.

When deciding whether there is '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
- undermine the safe environment of the school or disrupt teaching
- commit an offence.

If inappropriate material is found on the device, it is up to the DSL or other member of the Senior Leadership Team 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 if 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
- the student 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 DSL (or equivalent) immediately, who will decide what to do next. The DSL 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 students 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](#)
- The school's Behaviour Policy.

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

6.4 Artificial intelligence (AI)

Generative Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Our school recognises that AI has many uses to help students 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.

Walthamstow School for Girls will treat any use of AI to bully students in line with our school's Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Staff will not use AI tools to support work involving the use of personal data.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All students, parents/carers, staff, volunteers and governors, where they would be using the school ICT system, are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices A and B). 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and will restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices A and B.

8. STUDENTS USING MOBILE DEVICES IN SCHOOL

Students may not use mobile devices and other banned items in school in accordance with the school's Behaviour Policy.

9. STAFF USING WORK DEVICES OUTSIDE OF 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
- 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 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 B.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager or Technician.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our school's 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.

11. TRAINING

11.1 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 e-mails, 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, 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 to

- develop better awareness to assist in spotting the signs and symptoms of online abuse

- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL deputies 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 Safeguarding Policy.

11.2 Pupils

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
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

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

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found here [Senso Support | Cloud Classroom and Network Management Solution](#)

This policy will be reviewed every year by the SLT member with oversight of ICT. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. LINKS WITH OTHER POLICIES

This Online Safety Policy is linked to our:

- Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy

APPENDIX : A

KS2, KS3 and KS4 Acceptable Use Agreement (for students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (computers, iPads or any school devices) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or another member of staff) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

APPENDIX B

Acceptable Use Agreement (for Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of students without checking with teachers first
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

APPENDIX C

Online Safety Training Needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	