Windsor Academy Trust

(Newcastle Academy)

E-Safety Policy	
Responsible Committee:	**Education Performance and Standards Committee**
Implementation date:	**May 2024**
Next review date:	**May 2028**

DOCUMENT CONTROL	
VERSION NUMBER:	V1.0
POLICY STATUS:	Statutory
POLICY TYPE:	Trustwide
REQUIRED TO PUBLISH:	Yes
POLICY LEAD:	Director of Education

VERSION CONTROL		
VERSION	**DATE**	**CHANGES**
V X.X *	02.07.26	SCHEDULED REVIEW

1. Introduction

1.1 Windsor Academy Trust (WAT) has outlined its commitment to safeguarding and promoting the welfare of all students in its Child Protection and Safeguarding and Health and Safety policies. Safeguarding determines the actions taken to keep children safe and protect them from harm in all aspects of their school life to ensure that they have the best outcomes. This is underpinned by a culture of openness where both children and adults feel secure, able to talk, and believe that they are being listened to.

1.2 Windsor Academy Trust is committed to: fulfilling its moral and statutory responsibility, ensuring that robust procedures are in place, outlining the actions that it will take to prevent harm, to promote well-being, to create safe environments and to respond to specific issues and vulnerabilities.

1.3 WAT will meet its commitment by:

- Having robust processes and a clear overview of roles and responsibilities in place to ensure the online safety of students, staff, volunteers, directors and Local Community Committee representatives;
- Delivering an effective approach to online safety, which empowers WAT to protect and educate the whole WAT community in its use of technology;
- Establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Purpose

2.1 The purpose of this policy is to safeguard students, staff, volunteers, Local Community Committee representatives and directors from the many issues that can arise as a result of using electronic media.

3. Compliance with Legislation and Guidance

3.1 This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. The Windsor Academy Trust's Filtering and Monitoring Roles and Responsibilities document is in line with the DfE standards.

3.2 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.

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

4. Compliance with related policies and agreements

4.1 This policy complies with WAT's funding agreement and Articles of Association.

4.2 This online safety policy is also linked to the following WAT policies:

- Child Protection and Safeguarding
- Health and Safety
- Information Security and Acceptable Use
- Behaviour (Code of Conduct)
- Disciplinary
- Data Protection and privacy notices
- Complaints Policy

4.3 It should also be read in conjunction with academy student behaviour policies and procedures.

5. Governance Board of Directors

5.1 The Board of Directors (BoD) has overall responsibility for monitoring this policy and for holding the WAT Executive Team and Headteachers to account for its implementation. WAT has a designated Director who oversees the governance arrangements for safeguarding and liaises with the Director of Education, Head of Student Services and Head of Safeguarding. The governance arrangements are outlined further in WAT's Child Protection and Safeguarding Policy and also references the WAT Health and Safety policy which should also be referred to in conjunction with this policy.

Local Community Committees

5.3 The Local Community Committee will:

- Ensure that they have read and understood this policy;
- Agree and adhere to the terms on acceptable use of WAT's ICT systems and the internet (appendix 2);
- Discharge their responsibilities outlined in the Scheme of Delegation and LCC Terms of Reference.

The Headteacher

5.4 The headteacher is accountable to the Chief Executive Officer and the BoD and is responsible for ensuring that staff understand this policy and for its consistent and effective implementation in their academy.

The Designated Safeguarding Lead (DSL)

5.5 The details and roles of each academy's DSL are set out in WAT's Child Protection and Safeguarding policy.

5.6 The DSLs have lead responsibility for online safety, in particular:

- Supporting the headteacher in ensuring that staff and volunteers understand this policy and that it is being implemented consistently throughout the academy and across WAT;
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 4) 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 academy's behaviour policy;

- Updating and delivering staff training on online safety (Appendix 3 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 academies to the headteacher ~~and/or Local Advisory Bodies;~~
- Reviewing and actively responding to filtering and monitoring reports.

5.7 This list is not intended to be exhaustive.

The ICT Manager

5.8 The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students and staff safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- WAT IT Team to conduct a monthly health check on the filtering and monitoring software to ensure it is working correctly;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Undertake an annual review of the WAT systems, processes and procedures against the DfE Filtering and Monitoring standards to offer assurance to Directors.
- The four standards identified by the DfE are:

- You should identify and assign roles and responsibilities to manage your filtering and monitoring systems.
- You should review your filtering and monitoring provision at least annually.
- Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.
- You should have effective monitoring strategies that meet the safeguarding needs of your academy or college.

5.9 This list is not intended to be exhaustive.

Directors, LCC representatives, staff, and volunteers

5.10 All staff, including contractors, agency staff, volunteers, directors and **LCC** representatives are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of WAT's ICT systems and the internet (Appendix 2) and in accordance with WAT's Information Security and Acceptable Use Policy, and for ensuring that students follow the terms on acceptable use (Appendix 1 and Appendix 5);
- Working with the DSLs to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy.

5.11 This list is not intended to be exhaustive.

Parents/Carers

5.12 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 ICT systems and internet (Appendix 1).

5.13 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: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Resources for parents and carers, Childnet International: https://www.childnet.com/resources/parents-and-carers

Visitors and members of the community

5.14 Visitors and members of the community who use WAT'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 (Appendix 2).

6. Educating students about online safety

6.1 The safe use of social media and the internet will also be covered in relevant subjects and the academy will raise students' awareness of the dangers that can be encountered online and may, for example, invite speakers to talk to students about this.

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

6.3 In **Key Stage 1**, students will be taught about how 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.

6.4 In Key **Stage 2**, students will be taught how to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact.
- WAT PSHE KS3 Curriculum - online harms and risks/dangers associated with AI
- WAT IT Curriculum - Year 9 - Ethical use of AI

6.5 In **Key Stage 3**, students will be taught how 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.

6.6 Students in **Key Stage 4** will be taught how to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- Report a range of concerns.

6.7 Students in **Key Stage 5** will be taught how to:

- Live safely in an online and connected world protecting their privacy; protecting their 'online presence';
- Appreciate how social media can expand, limit or distort their view of the world;
- Set and maintain clear boundaries around their personal privacy; protect their online privacy and identity.

7. Educating parents/carers about online safety

7.1 WAT will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via WAT websites or any virtual learning environment (VLE) and this policy will also be made available to parents/carers.

7.2 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.

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

8. Cyber-bullying

8.1 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.

Preventing and addressing cyber-bullying

8.2 To help prevent cyber-bullying, WAT will ensure that students understand what it is and what to do if they become aware of it happening to them or others. WAT 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.

8.3 The academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

8.4 Tutor group/class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

8.5 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.

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

8.7 The academy also provides information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

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

9. Online sexual harassment

9.1 We take sexual harassment or any type of inappropriate sexualised behaviour online very seriously. Our child protection and safeguarding policy follows DfE's statutory guidance, Keeping Children Safe in Education (KCSIE). This policy clearly sets out how incidents of such nature will be managed. All Windsor Academy Trust schools teach age-appropriate content about the sorts of online behaviours that are unacceptable and students are given clear guidance of how to report incidents if they arise.

10. Examining electronic devices

10.1 WAT staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

10.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules

10.3 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

10.4 Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

10.5 Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the WAT's Complaints policy.

11. Acceptable use of ICT systems

11.1 All students, parents/carers, staff, volunteers, directors and LCC representatives are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

11.2 Students involved in the 1:1 digital learning approach must sign the relevant acceptable use agreement set out in Appendix 5.

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

11.4 WAT will monitor the websites visited by students, staff, volunteers, directors, LCC representatives and visitors (where relevant) to ensure they comply with the above.

11.5 More information is set out in the acceptable use agreements in Appendices 1 and 2.

12. Students using mobile devices in school

12.1 Mobile phones are not permitted to be used at all during the school day including:

- Lessons
- Break time/lunch time
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

13. 1:1 Digital Learning Devices

13.1 Students using a device within our 1:1 approach must adhere to the guidance set out in the acceptable use agreements (appendix 5).

13.2 WAT academies will use an agreed e-safety system to monitor and filter content accessed at school and at home. This will ensure that students are kept safe from potentially harmful or inappropriate content.

14. Staff using work devices outside of WAT

14.1 Staff members using a work device outside of WAT must not install any unauthorised software on the device and must not use the device in any way which would violate the terms of acceptable use, as set out in the WAT Information Security and Acceptable Use policy and Appendix 2 of this policy.

14.2 Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of WAT.

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

14.4 Where a staff member misuses WAT'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 WAT's Disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

14.5 WAT will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

15. Training

15.1 The DSLs will complete regular child protection and safeguarding training as outlined in the WAT Child Protection and Safeguarding policy. The training will also include online safety, at least every 2 years. The DSLs will update their knowledge and skills on the subject of online safety at regular intervals, and at least annually and will ensure that all staff are trained and up to date with policies and procedures.

15.2 Training will be provided to DSLs on the use of filtering and monitoring systems used within WAT.

15.3 IT staff are to ensure they are capable of undertaking audits of filtering and monitoring systems.

15.4 WAT will be assured that each academy complies with training requirements as defined in KCSIE 2025. All staff will undergo safeguarding and child protection training at induction on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

15.5 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).

15.6 Directors and LCC members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

15.7 Volunteers will receive appropriate training and updates, if applicable.

16. Monitoring arrangements

16.1 The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 4.

16.2 This policy will be reviewed and agreed as a minimum on a biennial basis and in conjunction with the Child Protection and Safeguarding policy. This may be more frequent if national guidance requires ensuring that key statutory requirements are incorporated.

17. Filtering and Monitoring System

17.1 WAT use the London Grid for Learning (LGfL) Internet Service Provider (ISP) filtering system which meets all educational standards and is one of the leading educational ISP offerings in the country. All mandatory filtering is completed and in place through the provision. In addition to this, all WAT devices are using a combination of Securly and Senso to monitor all mobile and app content in addition to just web searching and filtering. Securly protects all WAT devices and is monitored by and external team, with alerts going to relevant, trained staff members.

17.2 To ensure colleagues have the level of understanding and the ability to effectively use the filtering and monitoring systems, training is made available by the service providers via face to face training and online content.

17.3 To ensure we continually comply with the DfE standards, we ensure annual reviews are undertaken to ensure our systems and processes remain robust and offer high levels of assurance and protection. Regular (monthly) audits and assessments are conducted to evaluate the effectiveness of the filtering and monitoring systems. Solution specific reviews are conducted on an ongoing basis by the Head of Digital Transformation and IT.

17.4 WAT have assigned roles and responsibilities (Appendix 6) for filtering and monitoring within the Trust and academies to ensure a clear understanding of who is responsible for ensuring compliance and best practice at differing levels.

Appendix 1
Acceptable Use Agreement (students and parents/carers)

Acceptable use of the ICT systems and internet provided by Windsor Academy Trust (WAT)	
Name of student:	
When using WAT ICT systems and accessing the internet in the academy or on any other WAT premises I will not: ● Use them for a non-educational purpose ● Use them without a teacher being present, or without a teacher's permission ● Access any inappropriate websites ● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) ● Use chat rooms ● 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 ● Share my password with others or log in to the academy's network using someone else's details ● Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer ● 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 the academy:** ● 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 understand that the Trust will monitor the websites I visit.** **I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.** **I will always use the ICT systems and internet responsibly.**	
Signed (student):	**Date:**

Parent/carer agreement: I agree that my child can use the ICT systems and internet provided by Windsor Academy Trust (WAT) when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the WAT 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 2
Acceptable Use Agreement (directors, LCC representatives, staff, volunteers, directors, and visitors)

Acceptable use of the ICT systems and internet provided by Windsor Academy Trust (WAT)
Name of Director, LCC representatives, staff/volunteer/visitor:
When using ICT systems provided by Windsor Academy Trust (WAT)and accessing the internet on WAT premises or using WAT devices, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature ● Use them in any way which could harm the reputation of the Trust ● 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 ● Share my password with others or log in to the WAT network using someone else's details
I will only use WAT ICT systems and access the internet on WAT premises or outside on a WAT device, for educational purposes or for the purpose of fulfilling the duties of my role. I understand that WAT will monitor the websites I visit. 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 WAT Data Protection Policies including the Information Security and Acceptable Use 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 WAT's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (Director, LCC representative, staff/volunteer/visitor):	**Date:**

Appendix 3
Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in your academy?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the WAT acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
Do you regularly change your password for accessing the WAT ICT systems?	
Are you familiar with WAT's approach to tackling cyber-bullying?	

Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4 - Online Safety Incident Report Log

(*To be completed if information not captured on electronic recording system)*

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 5

1:1 iPad Digital Learning – Acceptable Use Agreement

Student Agreement

I understand that this agreement applies to use of the iPad both inside and outside school and that all rules apply at all times.

- I will take good care of the iPad, case and any accessories provided, or any loan devices.
- I will never leave the iPad unattended in an unsafe place.
- I will use the iPad responsibly, safely and ethically.
- I will never lend the iPad to other individuals or allow my iPad to be switched for another.
- I will know where the iPad is at all times.
- I will ensure that the iPad is out of sight when/if using public transport.
- I will keep food/drink away from the iPad.
- I will not deface the iPad, its case or remove any labelling.
- I will not take apart any part of the iPad, the case or attempt any repairs.
- I will protect the iPad by only carrying/using it while in the case provided. I will not force the device into a locker, bag or desk as this may break the screen.
- I will bring the iPad fully charged into school so it is ready to use in lessons.
- I will only use the iPad at break or lunchtime if I am directed to do so by a teacher.
- I will only use the photo/video function of the iPad if directed to do so by a teacher and will never share these photos or videos.
- I will use the iPad in ways that are appropriate, meet the school's expectations and do not have a negative impact in the classroom.
- I understand that the iPad can be inspected at any time without notice.
- I will report it straight away if the iPad is lost, stolen or damaged.
- I will adhere to the 'strictly prohibited' activities outlined at the end of this document.
- I agree that I will not sign into any websites, software or accounts that are not appropriate for my age. What I sign into can be seen by the school.
- If I use entertainment apps, I will do so respectfully and appropriately, ensuring that my parents/carers are well aware of what I am logging into and using.
- I will not download films or other media directly to the device. If watching films or other media, I will do so using home or public WiFi.

Student's signature:

Date: _____

Parent/Carer Agreement

I understand that this agreement applies to the use of the iPad inside and outside school and that all rules apply at all times.

- I will ensure that my child cares for and respects the iPad, accessories and any loan devices.
- I will ensure that my child brings the device to school fully charged each day.
- I will ensure that my child uses the iPad in line with this document and all applicable laws.
- I will report any damage to the device promptly to school.
- I will report if the device has been lost or stolen to the school and the police immediately and obtain a crime reference number to aid in this investigation.
- I understand that if it's clear that my child has maliciously damaged the device or accessories, I will be charged for the cost of the repair or a replacement.
- I understand that where there has been accidental damage on more than one occasion, I may have to make a contribution to the cost of repair or replacement.
- It is intended that this agreement is provided to supplement and work to support the school's existing e-safety policy.
- If my child is found to be misusing the device in any way, they will be sanctioned in accordance with the school's behaviour policy.
- I understand that the iPad has monitoring and filtering software installed to protect my child from accessing potentially harmful online content. However, I still recognise the importance of making sure my child is using the device responsibly, safely and respectfully at school and at home.
- I will ensure that the device, case and accessories and/or any loan devices are returned to the school when my child leaves the school or at any time upon the request of a member of school staff.
- If my child loses or breaks the charging lead and plug, I will replace it.
- I will ensure that my child does not download films or other media directly to the device. If they are watching films or other media, they will do so on home or public WIFI.
- I agree to the Terms and Conditions as outlined on page 4 - 7 of this document.

Parents signature: _____

Date: _____

Appendix 6
WAT Filtering and Monitoring - Roles and Responsibilities

WAT Board	● The Audit and Risk Committee validate WAT's annual review of the DfE's filtering and monitoring standards on behalf of the Board of Trustees. ● Seek assurance that filtering and monitoring systems are robust, in line with policies and are keeping students safe online (via the Audit and Risk Committee)
Designated Director for Safeguarding (DDS)	● DDS will evaluate online safety (and filtering and monitoring) as it arises in the termly safeguarding strategy meetings, as well as through the chairing of the Audit and Risk Committee
Executive team Chief Operating Officer (COO)/ Strategic Safeguarding Lead (DoE)	● Provide the Board of Trustees (via Audit & Risk Committee) assurance that filtering and monitoring systems are robust, in line with policies and are keeping students safe online (COO) ● Ensure that WAT's annual review of the DfE's filtering and monitoring standards takes place robustly and that required actions are reflected in policy and implemented effectively. (COO) ● Ensure that Safeguarding audits evaluate online safety and monitoring effectively. (Director of Education as SSL) ● Ensure the Child Protection and Safeguarding and E-safety Policies are reviewed and updated, in line with DfE Filtering and Monitoring standards and KCSIE. (Director of Education as SSL)
Head of Student Services / Head of Safeguarding	● Carry out Safeguarding Audits that include checks on filtering and monitoring ● Monitor online safety and regularly review filtering requirements ● Update Child Protection and Safeguarding and E-Safety policies in line with DfE Filtering and Monitoring standards and KCSIE. ● Work closely with Headteachers / Executive Headteachers / Head of School and DSLs to ensure filtering and monitoring provisions are effective and incidents are acted on and recorded appropriately.
Head of Digital Transformation and IT / Data Analytics & 1:1 Device Lead	● Ensure monitoring and filtering systems and solutions are robust and inline with DfE standards ● Identify, implement and evaluate robust filtering and monitoring systems for WAT ● Documenting what is blocked or allowed, and why ● Ensure schools are kept up to date with training and implementation of filtering and monitoring systems ● Ensuring half termly audits of monitoring and filtering IT systems and software are completed and any actions completed.
Executive Headteachers / Headteachers / Head of School	● Work closely with the DSL and IT teams to evaluate the effectiveness of the provision, making sure that incidents are urgently picked up, acted upon and outcomes are recorded (on appropriate systems, e.g. CPOMs where it is a safeguarding concern) ● Receive filtering and monitoring reports to evaluate the effectiveness and robustness of systems in place. ● Make sure that key staff staff understand their role, are trained appropriately, follow policies, processes and procedures and act on reports and concerns
DSLs	● Review and actively respond to filtering and monitoring reports (delegated unless concerns are very serious) ● Provide a brief termly summary report to SLT ● Identify and swiftly resolve Safeguarding concerns, in line with WATs Child Protection and Safeguarding policy

Staff	• Must be clear on the expectations, the roles/responsibilities and systems used for filtering and monitoring
	• Must understand, respond to and report safeguarding and technical concerns, such as;
	  ◦ They witness or suspect unsuitable material has been accessed
	  ◦ They are able to access unsuitable material
	  ◦ They are teaching topics that could create unusual activity on the filtering logs
	  ◦ There is a failure in the software or an abuse of the system
	  ◦ There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
	  ◦ They notice abbreviations or misspellings that allow access to restricted material

Local Community Committees (LCC)	• Receive assurances that filtering and monitoring systems are keeping students safe within the HT LCC report safeguarding section as part of the termly HT update to LCC.
IT Teams	• Maintain and manage the filtering and monitoring system • Providing filtering and monitoring reports • Checking the system or completing actions following any concerns • Undertake half termly recording and reporting of Monitoring and Filtering Checks