Online Safety Policy
(including Filtering & Monitoring)

Policy area:	Operations & Safeguarding
Approved by:	CEO
Approval date:	25.11.25
Implementation date:	Immediate
Version:	V2
Review cycle:	Annual
Date of next review:	Autumn 26
Publication:	Public

VERSION CONTROL			
Version	**Date**	**Author/Reviewer**	**Substantive changes since the previous version**
DRAFT v0.2	August 24	DD/FMV(AIT)/GB	Policy to incorporate requirements for online safety and the procedures for recording & reporting of filtering and monitoring.
V1	Oct 24		Approved by GB (CEO) and FM (AIT) – Oct 24
V2	Nov 25	GB	Microsoft Form added throughout the document as the means of Reporting Online Safety Incidents to the CEO. Online Safety Incident Report Form (Fill in Form) Paras 3.3 – 3.5 amended to better reflect the role of trustees and governors and what is practicable Para 3.15 amended to include parental responsibility to read the AI Transparency Statement on school websites Para 6.17 amended to clarify that AI should not be used for pupil interaction Para 6.18 reworded to broaden scope to include the school community Para 6.19 amended to note the importance of approval process for proposed introduction of new Ais Para 8.4 amended to note the usage of Lightspeed software solution for filtering and monitoring Para 8.7 inserted to reflect cyberbullying of adults as well as pupils Para 11 – re-worded Added associated document – Risk Assessment for risks pupils face online

Contents

Appendices

(See Associated Forms for individual documents)

Appendix 1 – Filtering & Monitoring Checks (FORM ONE75-01)

Appendix 2 – Online Safety Concerns Incident Report Form (FORM ONE75-02) – hard copy version

Online Safety Incident Report Form (Fill in Form) – Microsoft Form

Appendix 3 – School/Trust Filtering & Monitoring Check (FORM ONE75-03)

Appendix 4 – Governor/Trustee Filtering & Monitoring Check (FORM ONE75-04)

Associated Documents

FORM ONE75-05 – Risk Register for risks pupils face online

1. Introduction

1.1 ONE Academy Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to protect learners and staff from potential harm online in the work environment.

1.2 This policy sets out our commitment to online safety and how we manage online safety within ONE Academy Trust, including our trust-wide arrangements for Filtering and Monitoring. Each of the schools within ONE Academy Trust has an online safety policy which operates at a local level.

1.3 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
- Filtering & Monitoring

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

1.5 This policy reflects existing legislation and guidance, including but not limited to:

- the Education Act 1996 (as amended)
- the Education and Inspections Act 2006 and the Equality Act 2010.
- the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- Filtering and monitoring standards for schools and colleges - the Department for Education (DfE)
- Establishing appropriate levels of filtering - the UK Safer Internet Centre
- Appropriate monitoring: guide for education settings and filtering providers - the UK Safer Internet Centre

1.6 This policy reflects legislation at the time when it was last reviewed. Any changes in legislation will take precedence over anything printed in the policy.

1.7 This policy complies with our funding agreement and articles of association.

1.8 This online safety policy is linked to our following policies:

- Acceptable Use of IT policy
- Each school's Child Protection and Safeguarding Policy
- Each school's Behaviour Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Codes of Conduct
- Extremism & radicalisation policy

2. Aims

2.1 One Academy Trust aims to:

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

The 4 key categories of risk

2.2 Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Roles and responsibilities

The Board of Trustees and Local Governing Bodies (LGBs)

3.1 The ONE Academy Trust Board of Trustees has overall responsibility for ensuring that appropriate and effective policies and procedures are in place to meet statutory requirements. They will hold the CEO and headteachers to account for its implementation.

3.2 Where a local governing body is established, governors hold responsibility for monitoring the implementation of this policy at a local level as part of the oversight of effective safeguarding. Where no local governing body is established, the board of trustees retains this responsibility.

3.3 The relevant governing board will also receive a report from the CEO/Headteacher to confirm that staff receive online safety training and regular updates (via email, e-bulletins and staff meetings), as required, to ensure staff have the skills and knowledge to effectively safeguard children

3.4 The relevant governing board will monitor the implementation of online safety in school(s) to ensure children are being taught how to keep themselves and others safe, including keeping safe online. This may include reports from the Headteacher/CEO, learning walks, and/or meeting with the DSL to discuss what provisions are in place. An optional form is available at Appendix 4 (Form ONE75-04) for governors to use for monitoring purposes and for 'spot checks'.

3.5 The Trust Board will ensure that the trust/school has appropriate filtering and monitoring systems in place on trust/school devices and trust/school networks, and will receive updates on their effectiveness. The board will review DfE filtering and monitoring standards and agree with senior leaders what measures are required to support the trust/school in meeting the standards. Measures will include:

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

- Ensure regular training is delivered to staff part of ONE Academy Trust
- The safeguarding link trustee will oversee trust-wide online safety provision. The Safeguarding Link Trustee is currently James Freeman. This may be subject to change whilst this version of the policy is extant. Please check the ONE Academy Trust website or contact the Governance Coordinator (d.dakin@oneacademytrust.co.uk) to confirm details.
- Each local governing board will appoint a governor who oversees online safety (including filtering and monitoring). This governor is usually the Safeguarding Link Governor. Please contact the school for details.

3.6 All trustees and governors will:

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet. See the Acceptable Use of IT Policy.
- Ensure that online safety is a running and interrelated theme while devising and implementing the trust-wide and school approach to safeguarding and related policies and/or procedures
- Ensure that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The CEO

3.7 The CEO (and/or a nominated member of the senior leadership team) will:

- Review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the trust and its schools in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Working with the IT provider (AIT) to make sure the appropriate systems and processes are in place
- Ensure that online safety is a running and interrelated theme while devising and implementing the trust-wide approach to safeguarding and related policies and/or procedures
- Review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Ensure that the workforce understand this policy, and that it is being implemented consistently throughout the trust.
- Ensure the workforce undertakes online safety training as part of child protection and safeguarding training, and ensure they understand the expectations, roles and responsibilities around filtering and monitoring.

The headteacher

3.8 The headteacher is responsible for:

- Ensuring that the workforce understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring that a school Online Safety Policy is published and reviewed regularly.
- Ensuring the workforce undertakes online safety training as part of child protection and safeguarding training, and ensure they understand the expectations, roles and responsibilities around filtering and monitoring.
- Ensuring all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are provided with the relevant skills and knowledge to effectively safeguard children.
- Ensuring that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Working with the DSL, ensuring that checks take place to ensure the filtering and monitoring systems are operating effectively and required actions are followed up. Suggested forms are available at Appendix 1 (programme & suggested checklist) and Appendix 3 (Form ONE75-03).
- Reporting to governors/trustees on the effectiveness of online safety and the filtering and monitoring systems.
- Review monthly filtering and monitoring reports regularly alongside the governing body, DSLs and appropriate Trust staff

The designated safeguarding lead (DSL)

3.9 The trust-wide DSL supports the CEO and headteachers in implementing and monitoring the effectiveness of online safety across the trust. Details of the trust-wide DSL are published on the trust website.

3.10 Details of each school's designated safeguarding lead (DSL) and their deputy/deputies are set out in the school's child protection and safeguarding policy and on the school website.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the headteacher, ensuring that regular checks and audits of the filtering and monitoring systems take place, are recorded and actions are followed up (see Appendix 1 (programme & suggested checklist) and Appendix 3 (Form ONE75-03) for supporting resources.

- Working with the ICT provider (AIT) to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and reported to the CEO online using the Online Safety Incident Report Form (see also Appendix 2 for details of content) and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour and anti-bullying policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and the governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The IT service provider

3.12 Our external IT service provider (AIT) is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on trust/school devices and trust/school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the trust and each school's ICT systems are secure and protected against viruses and malware, and that safety mechanisms are updated regularly
- Conducting a full security check and monitoring the trust/school's ICT systems on a **monthly** basis
- Blocking access to potentially dangerous sites, or those sites categorised as harmful in education in accordance with the UK Safer Internet Centre, and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and reported to the CEO online using the Online Safety Incident Report Form (see also Appendix 2 for details of content) and dealt with appropriately
- Provide regular reports to schools within the Trust and over-arching filtering and monitoring reports to ONE Academy Trust
- Provide annual training on filtering and monitoring in line with the latest governance and statutory guidance as applicable
- Immediately report any harmful activities that pose a safeguarding risk to staff or students within the Trust to the relevant parties

All staff and volunteers

3.13 All staff, including contractors and supply staff, and volunteers are responsible for:

- Reading, understanding and implementing this policy and (where appropriate to role) the school's online safety policy
- Agreeing and adhering to the terms on the Acceptable Use of the trust/school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Ensuring that any online safety incidents are logged and reported to the CEO online using the Online Safety Incident Report Form (see also Appendix 2 for details of content) and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

Parents/carers

3.14 Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child understands the rules about using the school's ICT systems and internet
- Read the school's Artificial Intelligence Transparency Statement published on school websites

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

- **What are the issues? – UK Safer Internet Centre**
- **Hot topics – Childnet**
- **Parent resource sheet – Childnet**

3.16 More guidance and information for parents/carers is available on each school's website and each school's online safety policy.

Visitors and members of the community

3.17 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see the Acceptable Policy).

4. Educating pupils about online safety

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

4.2 The text below is taken from the National Curriculum computing programmes of study and from the guidance on relationships education, relationships and sex education (RSE) and health education.

4.3 All schools have to teach:

- **Relationships education and health education** in primary schools

4.4 In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

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

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

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

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

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

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

5. Educating parents/carers about online safety

5.1 Each of our schools will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

5.2 Online safety will also be covered during parents' evenings.

5.3 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

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

6. Cyber-bullying

Definition

6.1 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. (see also the school behaviour policy.)

Preventing and addressing cyber-bullying

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

6.3 Our schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

6.4 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.

6.5 All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see paragraph 10 for more detail).

6.6 In relation to a specific incident of cyber-bullying relating to pupils, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.7 Instances of cyber bullying or harassment relating to adults will be dealt with under the relevant trust wide staff policies and procedures (e.g. Codes of Conduct, Bullying and Harassment Policy, Disciplinary Procedures)

Examining electronic devices

6.8 The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school's behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/ DSL.

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

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

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

6.13 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, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

6.14 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

6.15 Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's behaviour policy/searches and confiscation policy

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

Artificial intelligence (AI)

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

6.18 ONE Academy Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others and for data security to be compromised. Therefore, the Trust does not currently support the use of AI for pupil interactions.

6.19 ONE Academy Trust will treat any use of AI for bullying and harassment purposes against members of the school community in line with the trust and school's relevant policies e.g. Codes of Conduct and Disciplinary procedures.

6.20 Staff should be aware of the risks of using AI tools whilst they are still being developed, and a risk assessment should be carried out where new AI tools are to be used by the school/trust. Any software to be used/downloaded onto trust/school devices must be subject to prior approval in accordance with the Acceptable Use of IT policy and the Trust's Use of AI Policy and must be included in the Trust's AI Risk Register.

7. Acceptable use of IT Policy (including use of social media)

7.1 All pupils, parents/carers, staff, volunteers, trustees and governors are expected comply with the trust's Acceptable use of IT Policy. Visitors will be expected to read and agree to the school's terms on acceptable use of IT if relevant to their activities.

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

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

7.4 More information is set out in the ONE Academy Trust Acceptable Use of IT policy.

8. Filtering & Monitoring

What is filtering and monitoring?

Filtering and monitoring systems are used to keep staff and pupils safe when using our school's IT system.

- Filtering is the safety measure designed to restrict and control the content which can be accessed by staff, pupils, volunteers, and visitors. Filtering systems block access to harmful sites and content.
- Monitoring concerns the review of user activity on the school's network to promote the safeguarding of staff, pupils, volunteers, and visitors. Monitoring systems identify when a user accesses or searches for certain types of harmful content on school/trust devices (it doesn't stop someone accessing it). The school/trust is then alerted to any concerning content so that the school/trust can intervene and respond.

8.1 All staff should be clear on:

- The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens
- How to report safeguarding and technical concerns, such as if:
  - 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 failure in the software or 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

8.2 Senior leaders and all relevant staff need to be aware of and understand:

- What provisions the trust/school has in place and how to manage these provisions effectively
- How to escalate concerns when they identify them

8.3 They are also responsible for:

- Buying-in the filtering and monitoring system for the trust/schools (this is actioned trust-wide as part of our IT strategy). Currently the Trust uses the 'Lightspeed' filtering software.
- Documenting what is blocked or allowed, and why
- Reviewing the effectiveness of provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded
- Overseeing reports
- Making sure staff are trained appropriately and understand their role

8.4 The DSL should take lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place – this is part of their role in taking the lead responsibility for safeguarding. This includes overseeing and acting on:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

8.5 Each school should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems (this is a function of the executive team)
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet your safeguarding needs
- Maintain a record (folder) of all filtering and monitoring checks, audits, training and changes.

8.6 We have an obligation to put in place suitable Filtering and Monitoring systems. These apply to our devices, whether used on site or off site. Filtering and Monitoring will also apply to personal devices that access our internet connection on the site.

Unblocking sites

8.7 Staff can request sites to be unblocked. Requests should be emailed to the DSL, headteacher and/or IT coordinator as applicable to the setting. The request should include the following information. A record of the request will be held with the Filtering and Monitoring Log.

- Staff name and year group/department:
- Website title and URL/link:
- Year group you want the website unblocked for (if applicable):
- Reason why you want the website unblocked:
- Can we re-block this site after a specific date?

9. How the trust/school will respond to issues of misuse

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

9.2 Where a member of the workforce or volunteer misuses the trust/school's ICT systems or the internet, or misuses a device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures (employees), the relevant code of conduct and the ONE Academy Trust Acceptable use of IT policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

10. Training

10.1 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.

10.2 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).

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

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

10.4 Training will also help staff:

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

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

10.5 The DSL and deputy/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.

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

10.7 Volunteers will receive appropriate training and updates as applicable to their role.

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

11. Monitoring & review

11.1 This policy will be reviewed annually by the CEO.

11.2 Periodically, the trust will conduct an online safety review alongside the Trust's IT providers (such as the one available here). This will be supported by a risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendices

Filtering & Monitoring Checks & Audit

Check	Responsibility
Weekly	
Filtering and Monitoring systems functioning as expected	AIT
Ensure any websites for lessons for the upcoming week are available or request them to be unblocked	Headteacher/DSL
Monthly	
Filtering and Monitoring Reports to be sent to the nominated contacts within the Trust	AIT
Review monthly reports and follow up on any concerns	Headteacher/DSL
Termly	
Filtering & Monitoring Check (school) Test a random selection of at least 2 devices onsite, accessing websites that would typically be blocked to ensure no access. Report findings to IT and governors	Headteacher/DSL
Suggested Filtering & Monitoring Check (governors) Nominated governor	
Ongoing	
Act appropriately to any evolving risks, blocking of websites or change in altering levels with Filtering and Monitoring systems in school	AIT & Headteachers/DSL/All Staff
Ad-hoc	
Monitoring alert triggers reviewed and acted upon appropriately when they arise from the monitoring solution	Headteacher/DSL

Appendix 2
FORM ONE75-02

Online Safety Incident Report Form

Please report to the CEO by completing the Microsoft Form Online Safety Incident Report Form

This appendix details the content required on the Microsoft Form and you may wish to complete this hard copy version to retain for local records.

Name of school/trust	
Name of lead person who dealt with the incident	
Date of the reported incident	
What threshold level was the incident classified as on Lightspeed? (2, 3 or other)	
Where the incident took place e.g. area of the school, working from home	
Provide details of the incident e.g. year group, adults involved, nature of the incident, any related information	
Action taken (e.g. who was notified, any changes made as a result, sites blocked/unblocked, any new checks made, safeguarding logs updated)	

A copy of the Incident Report Form should be filed and retained in the school/trust Incident Log (e-version and/or hard copy)

Dealing with an incident

Please follow your normal safeguarding, whistleblowing and LADO procedures. If you are aware of an incident where monitoring or filtering has failed or highlighted a problem, please consider the following:

- do you need to get the website blocked
- check who has/had access
- if this could be disciplinary, what are you legally obliged to do? (NB: this could be different depending on the issue)

Remember to record what you decide to do and any changes you make.

Filtering & Monitoring Check (school/trust)

Name of school/trust	
Name & role of person completing the check	
Date of check	

Suggested checks (what was tested) *(select from list below or insert detail of additional checks)*	**Check completed**	**Concerns & actions arising** *Continue on additional page and include screenshots as required*
Do the current filtering and monitoring provisions meet the risk profile of our pupils? E.g. EAL, age, high level of refugees and asylum seekers, high level of SEND/ASD, outside influences e.g. County Lines, Prevent duty *Detail risk profile below*:		
What sites are currently blocked and what sites have different levels of access for users? *(AIT to provide)* Are these still appropriate? Do any changes need making?		
Are blocked sites still blocked?		
Have any new devices been added?		
Have any user groups changed?		

Suggested checks (what was tested) *(select from list below or insert detail of additional checks)*	**Check completed**	**Concerns & actions arising** *Continue on additional page and include screenshots as required*
Is Google Safe search on?		
What are the YouTube settings?		
Check search history on different devices. (see below)		
Check key words *(particularly around local issues e.g. county lines etc.)* *List words below*:		
Check for recent online trends (TikTok style challenges etc.) *List below*:		
Safeguarding issues/reports *List below*:		
Any common issues pupils have been having outside of school *List below*:		
Filtering Checks *(see log below):* Examples: Safe Search is working and not able to access YouTube Checking access to site used for lesson is allowed Is teacher allowed to access personal TikTok account on school laptop Run Testing Tool to check filtering is blocking access Filter a weblog for key words		

Suggested checks (what was tested) *(select from list below or insert detail of additional checks)*	**Check completed**	**Concerns & actions arising** *Continue on additional page and include screenshots as required*
Check curriculum sites that are required (RSE, PSHE etc.)		
Does the filtering allow you to identify the device ID (IP address)?		
Does the filtering allow you to identify the date and time of the attempt blocked?		
Does the filtering system handle misspellings and abbreviations? Are there any known slang words you could check? *List below*:		
Does the filtering system handle slang, emojis and foreign languages?		
Do staff connect their own devices to the school wif-fi? If so, how is this monitored? Are there any incidents of misuse?		
Are you satisfied that your filtering system is blocking all of the following? Child sexual abuse material (CSAM), Extremism & Radicalisation, Gambling, Pornography, Discrimination, Piracy and copyright theft, Self-harm, Violence, Malware/hacking, Drugs/substance abuse		
Monitoring checks *(see log below)* Examples: Review logfile Look at images on a device Look at internet history of device Check access to a few websites that are blocked		
Do staff physically monitor the use of devices? (e.g. actively checking what the pupils are doing on their devices during the lessons)		
Do staff know how to deal with any incidents?		

Suggested checks (what was tested) *(select from list below or insert detail of additional checks)*	**Check completed**	**Concerns & actions arising** *Continue on additional page and include screenshots as required*
Do staff know who to contact?		
When did staff last have a training? (Dates) Have all staff completed the training?		

Filtering & Monitoring Log				
Date checked:				
Checks conducted by:				
Device	**Location** (e,g. classroom or staffroom)	**Logged in as** (pupil/staff etc.)	**Check conducted**	**Result (Including actions arising)**
Filtering System				
Monitoring System				

Reported to Designated Safeguarding Lead and headteacher	**Date:**
Reported to Local Governing Body and/or Board of Trustees	**Date:**

Filtering & Monitoring Check (governors/trustees)

Name of school/trust	
Name & role of person completing the check (governor/trustee)	
Date of check	

Suggested checks *(select from list below or insert details of additional checks)*	**Check completed**	**Concerns & actions arising** *Continue on additional page and include screenshots as required*
The termly report received from the school/trust confirms that: a. Filtering & monitoring checks are being undertaken b. Actions are being followed up and issues addressed		
Filtering & monitoring checks are being undertaken by the IT service provider (AIT) and actions are followed up and issues addressed.		
A filtering & monitoring lead governor/trustee is in post and is being kept aware of any major issues arising		
Staff training is up-to-date		
Are you satisfied that your filtering system is blocking all of the following? Child sexual abuse material (CSAM), Extremism & Radicalisation, Gambling, Pornography, Discrimination, Piracy and copyright theft, Self-harm, Violence, Malware/hacking, Drugs/substance abuse *Take into account the school report and governor checks.*		

Filtering & Monitoring Log				
Date checked:				
Checks conducted by:				
Device	**Location** (e,g. classroom or staffroom)	**Logged in as** (pupil/staff etc.)	**Check conducted**	**Result (Including actions arising)**
Filtering System				
Monitoring System				