DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

SNMAT

eSafeguarding Policy

Policy:	eSafeguarding / eSafety Policy
Approved by:	SNMAT Board of Directors
Date:	July 2026
Review Cycle:	Annual

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2020	March 2020	DO – IT Director	Initial version.
2021	April 2021	DO – IT Director	No changes.
2022	May 2022	BD & TTL	Changed IT Director to Trust Technical Lead. IT Technical Guidance and Cyber Security Policy added to links with other policies. Paragraphs numbered throughout the policy.
2023	April 2023	MJH – IT Coordinator	e-Safety to eSafeguarding Redesign of document. Split policy rationale into individual statements. Added Keeping Children Safe In Education (2022) Statutory Guidance references throughout. Added Meeting Digital Technology Standards in Schools and Colleges (2023) guidance references throughout. Added DSL as co-responsible of management and operation of eSafeguarding policy and updated responsibilities. Removed responsibility of IT Support to evaluate the effectiveness of senior staff role responsibilities. Added use and functionality of classroom management tools throughout the policy. Expanded Trust IT Teams and IT Service Provider responsibilities. Added parental responsibilities for ensuring children's personal devices, social media usage and internet connections are home at filtered and configured with parental controls.

			Added Removing Evidence from Digital Devices guidance for staff and IT Support teams. Added Emerging Technologies appreciation. Added Internet Access section covering filtering configurations. Removed responsibility from IT Support Teams for active monitoring of filtering reports. Added Microsoft 365 section.
2024	May 2024	MJH – IT Manager	Updated references to DfE Keeping Children Safe in Education (2023). Updated references to DfE Meeting Digital and Technology Standards in Schools and Colleges for its update in January 2024. This includes an update to digital leadership and governance. Added specific responsibilities in regard to filtering and monitoring to DSL/Headteacher/Principal. Added responsibilities for the SLT member responsible for digital technology throughout. Added references to Artificial Intelligence. Added parents and student responsible use of Social Media. Included reporting concerns via The National Cyber Security Centre. Added use of Lightspeed and Securly as secondary internet filtering solutions and their ability to automate safeguarding alerts and reports. Added policies for managed devices. Minor grammar and spelling changes.
2024.1	June 2024	MJH – IT Manager	Reviewed in-line with draft to DfE Keeping Children Safe in Education (2024) released by the DfE on 24 May 2024.

			Added extra staff responsibilities re: paragraph 22. In KCSIE 2024. Added 21 and 38 to reflect that as part of a DSLs annual review it should include filtering and monitoring provision. Amended 45, that owners of Teams or SharePoint sites are responsible for their content, shared links, etc. Amended 48 that student webcams are also restricted in policies. Amended 49 to Searching, Screening and Confiscation in Schools guidance. Amended 33 to reference specific Online Safety-Advice Annex.
2025	April 2025	MJH	References to updated DfE Meeting Digital and Technology Standards in Schools and Colleges.
2025.7	July 2025	MJH	Updated references to KCSIE 2025. Added EXA SurfProtect as filtering and monitoring option in schools. Internet Access updated to reflect Page 38, Paragraph 135 of KCSIE 2025: Misinformed, Disinformation and Conspiracy Theories included as safeguarding harms. Added new section on Artificial Intelligence, referencing the MAT guidance and Page 41, Paragraph 143 of KCSIE 2025. Use of Generative AI in Education. Updated annual review paragraph for KCSIE 2025.
2026	Mar 2026	MJH	Modified Internet Content. Amended DSL responsibilities. Added reliably identifying users into Testing, Reporting and Monitoring. Added AI into Testing, Reporting and Monitoring. Added AI into Internet Access.

			Office 365 changed to Microsoft 365. Added DfE AI guidance in AI. Added reference to Microsoft Teams policies.
2026.7	July 2026	MJH	Updated references to KCSIE 2026 throughout. A few spelling fixes. Updated reference to KCSIE (2026) paragraph 173 for DSLs to carry out an annual review of their approach to online safety, and review filtering and monitoring provision. Updated reference to KCSIE (2026) paragraph 166 stating schools should follow DfE Using Generative AI in Education and Trust Artificial Intelligence (AI) Guidance to use AI effectively and safely. Added Google Workspace as one of the recommended T&L platforms and the expected safeguards that should be in place.

EXECUTIVE SUMMARY

1. The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in academies are bound. Academies must, through their eSafeguarding Policy ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside the academy. The policy also forms part of the Trust's/academy's protection from legal challenge, relating to the use of digital technologies.

SCOPE

2. This policy applies to all members of the Trust/Academy community (including staff, pupils/students, volunteers, parents / carers, visitors, community users) who have access to and are users of Trust/Academy IT systems.

RATIONALE

3. The Education and Inspections Act 2006 empowers Principals/Headteachers to such extent as is reasonable, to regulate the behaviour of pupils/students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other eSafeguarding incidents covered by this policy, which may take place outside of the academy, but are linked to membership of the trust/academy.

4. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data if the Principal/Head Teacher believes it contains any material that could be used to bully or harass others or used to commit a crime.

5. The DfE Keeping Children Safe in Education (2026) statutory guidance provides clear instruction to academies to take an effective whole school approach to ensuring that children are safeguarded from potential harm and inappropriate material online.

6. The Government's Meeting Digital and Technology Standards in Schools and Colleges (last updated June 2026) outlines standards of digital leadership and governance and provides guidelines for schools to provide a safe environment to learn and work when online.

7. The Counter Terrorism and Securities Act 2015 requires academies to ensure that children are safe from terrorist and extremist material on the internet.

8. Each Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate eSafeguarding behaviour that take place out of school.

OBJECTIVES

The SNMAT eSafeguarding Policy aims to:

9. To educate all SNMAT stakeholders to take a responsible approach to eSafeguarding;

10. To help and support children and young people to recognise and avoid online safety risk and build their resilience:

11. To reinforce eSafeguarding messages and make eSafeguarding a focus in all areas of the curriculum;

12. To provide information and awareness to parents to help them understand these issues through parents' evenings, all communication channels and provide information about national/local online safety campaigns/literature;

13. To provide effective eSafeguarding training and guidance for staff to ensure they understand their responsibilities;

14. To ensure that children are safeguarded from potential harmful and inappropriate material online as required by the Keeping Children Safe In Education (2026) statutory guidance.

15. To ensure that children are safe from terrorist and extremist material on the internet as required under the Counter Terrorism and Securities Act 2015.

ROLES AND RESPONSIBILITIES

Board of Directors

16. The Board of Directors is accountable for the effective operation of the eSafeguarding policy overall. Regular reports around safeguarding in the academies are received by the Board. These include reference to eSafeguarding where appropriate.

Local Governing Body

17. The responsibility for the effective operation of the policy in Academies has been delegated to the Local Governing Body who will monitor and review its operation by receiving regular reports about eSafeguarding incidents and monitoring filtering and change control logs. It is suggested that the Safeguarding Governor includes the monitoring of eSafeguarding within their remit.

Principal/Headteacher and Designated Safeguarding Lead

18. The responsibility for the day-to-day operation of the eSafeguarding policy has been delegated to the Principal/Headteacher and DSL. The Principal/Headteacher and DSL is responsible for:

    - Shaping and applying this policy;
    - Ensuring that all the staff have read and understand the policy;
    - Ensuring that staff receive regular, relevant and suitable training and continued development to enable them to carry out their roles using IT;
    - Ensuring that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident taking place;
    - Meeting Keeping Children Safe in Education (2026) and DfE Meeting Digital and Technology Standards In Schools and Colleges expectations for understanding filtering and monitoring, assisting with procurement and reviewing alerts and monitoring for configuration and effectiveness;
    - Reviewing and responding to any eSafeguarding incidents escalated to senior leaders, as well as reviewing reports from the MAT's appropriate IT Teams and Service Providers;
    - Liaising with MAT/Academy/School IT Teams and Service Providers.

Staff

19. All staff are responsible for ensuring that:

    - They have an up-to-date awareness of eSafeguarding matters and of the current SNMAT eSafeguarding Policy and practices;
    - They have read, understood and signed any Academy Acceptable Use of IT Policy;
    - They are aware that technology is a significant component in many safeguarding and wellbeing issues;
    - They report any suspected misuse or problem to SLT, the Principal/Headteacher or DSL;
    - They embed eSafeguarding into all aspects of the curriculum and other school activities wherever possible;
    - Pupils/students understand and follow the eSafeguarding Policy and Academy Acceptable Use Policy;
    - Pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to the age of the pupils/students;
    - Use good classroom management and the provided classroom management software tools where available to monitor and manage the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
    - In lessons where internet use is pre-planned students/pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The Designated Safeguarding Lead

20. The Academy DSL should be trained in eSafeguarding issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

    - Sharing of personal data;
    - Access to illegal / inappropriate materials;
    - Inappropriate on-line contact with adults/strangers;
    - Potential or actual incidents of grooming;
    - Cyber-bullying.

Senior Leader Responsible For Digital Technology

21. The Academy Senior Leader Responsible for Digital Technology should:

    - Work with Principals/Headteachers, Designated Safeguard Leads and IT Support Teams to ensure eSafeguaridng is embedded in the Academy's Digital Technology Strategy.
    - Conduct an annual review of the Academy's approach to online safety that includes filtering and monitoring provision and reporting.

IT Support Teams & IT Service Providers

22. Academy IT Support Teams and Service Providers should:

    - Ensure that SNMAT IT infrastructure and devices are secure, compliant and not open to misuse or malicious attacks in-line with this guidance and policy;
    - Liaise with Academy/School DSL, SLT Digital Leads and Principals in providing technical assistance and expertise where appropriate.

Pupils/students

23. Pupils/Students are responsible for:

- Using the academy digital technology systems in accordance with the Pupil/Student Acceptable Use Policy;
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to their age – including the use of Artificial Intelligence (AI);
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Knowing and understanding policies on the use of mobile devices and digital cameras, taking and the use of images and video and the impact of illegal activities such as hacking and cyber bullying;
- Understanding the consequences of breaching eSafeguarding policies and why the policies are in place;
- Understanding the importance of good online safety when using digital technologies and social media platforms and realising that the Trust and Academy eSafeguarding Policies cover their actions out of school if related to their membership of the Academy.

Parents/Carers

24. Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet, computing, gaming and mobile devices in a responsible and safe way. Parents/carers will be encouraged to support SNMAT in promoting good eSafeguarding practises and follow guidelines on the appropriate use of:

    - Internet, computing, gaming and mobile devices at home, ensuring that children's internet connections are filtered, and devices and consoles are correctly configured with parental controls to restrict inappropriate age-related apps, social media, games and content;
    - Social media, and the use of digital and video images taken at school events;
    - access to parents' sections of the website/Learning Platform and on-line pupil/student records;
    - their children's personal devices in the academy (where this is allowed).

LINKING WITH OTHER POLICIES

25. The eSafeguarding Policy must be read in conjunction with the other following policies:

- Artificial Intelligence Guidance
- ICT Policy
- IT Technical Guidance
- Cyber Security Policy
- Bring Your Own Device (BYOD) Policy
- Data Protection Policy
- Social Media Policy
- Policy for Child Protection to Safeguard the Welfare of Children
- eSafeguarding – Microsoft Teams Student Policies

GUIDANCE FOR IMPLEMENTATION

Curriculum

26. The eSafeguarding curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited;
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities;
- Pupils/Students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information;
- Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils/students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils/students should be helped to understand the need for the Pupil/student Acceptable Use Policy and encouraged to adopt safe and responsible use of IT both within and outside the academy;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- Pupils/students should be guided to sites checked as suitable for their use in lessons where internet use is pre-planned;
- Processes should be in place for dealing with any unsuitable material that is found in internet searches;
- Staff should be vigilant in monitoring the content of the websites the young people visit where Pupils/students are allowed to freely search the internet;
- Pupils/students with special educational needs should be appropriately supported according to their specific needs and their personal understanding of the e-safety risks.

Parents/Carers

27. SNMAT and its Academies should seek to provide information and awareness to parents and carers through:

    - Curriculum activities
    - Social media, letters, newsletters, its web sites and learning platforms
    - Parents / Carers evenings / sessions
    - High profile events / campaigns e.g. Safer Internet Day
    - Reference to the relevant web sites / publications

Staff

28. SNMAT and its Academies should ensure that:

    - An audit of the eSafeguarding training needs of all staff should be carried out and a planned programme of formal eSafeguarding training made available to staff which is regularly updated and reinforced;
    - All new staff should receive online safety training as part of their induction programme including ensuring that they fully understand the SNMAT eSafeguarding Policy and Academy Acceptable Use Policy;
    - Staff identify eSafeguarding as a training need within the performance management process where appropriate;
    - The nominated person receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
    - The eSafeguarding Policy and its updates are presented to and discussed by staff in staff meetings/INSET days;
    - The nominated person provides advice/guidance/training to individuals as required.

Directors/Governors

29. The Trust/academy should ensure that:

    Directors/members of the Local Governing Body take part in eSafeguarding training/awareness sessions, particularly those who are members of any subcommittee/group involved in technology/online safety/health and safety/safeguarding.

INTERNET ACCESS

30. SNMATs internet web filtering policy has been developed to help our schools maximise the safety of our students as they use the internet, whilst at the same time retaining the flexibility needed for effective teaching and learning. The policy implements appropriate filtering that fulfils the DfE's statutory requirements for schools and colleges in regard to Keeping Kids Safe In Education (2026), DfE Meeting Digital and Technology Standards In Schools and Colleagues and PREVENT duties.

31. SNMAT appreciates that supervision and education in the use of the internet is paramount, and undertaken as part of our eSafeguarding training, as the filtering of internet connections alone cannot guarantee the absolute safety of students and staff. We do all that we reasonably can to limit children's exposure to the 4 areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: AI deepfakes, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact: being subjected to harmful online interaction with other users or AI chatbots, for example: abuse, coercive or controlling behaviour, dangerous stunts and challenges and fraud.
- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, 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. Concerns would be reported via The National Cyber Security Centre and Anti-Phishing Working Group.

Primary Filtering

32. SNMAT school internet connections are filtering using leading hardware and software manufacturer firewalls and filtering systems; Smoothwall, Sophos, FortiGate and EXA SurfProtect Quantum.

Secondary Filtering

33. Some Academies utilise additional filtering and classroom management tools such as Lightspeed, Smoothwall Cloud, Securly, Senso Cloud, Impero or AB Tutor that are fully compliant with the UK Safer Internet Centre's Appropriate Monitoring standards for schools, as referenced in the Online Safety-Advice Annex of the governments Keeping Children Safe in Education (2026) statutory guidance.

34. These tools monitor content accessed by staff and students and use a keyboard detection solution to monitor, capture, block and report inappropriate content. Impero for example develops its policies in conjunction with specialist organisations and charities, such as the Anti-Bullying Alliance, Beat, Hope Not Hate, the Internet Watch Foundation (IWF), the UK Government's Counter Terrorism Internet Referral Unit, iKeepSafe, Hey Ugly, and ANAD.

Bespoke Filtering

35. In line with the Goverments Meeting Digital and Technology Standards in Schools and Colleges Guidance, the responsibility for internet safety and the configuration of filtering lies with the Principal with support from SLT and DSL (the filtering solution can be tailored to meet the needs of individual schools if required) as administered by the school's IT Support Team.

36. KCSIE, Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) blocklists are mandatory and cannot be disabled or bypassed.

Managed Devices

37. Any Academy managed device will enforce restrictions to meet eSafeguarding and Internet Filtering and Monitoring requirements by deploying strict configuration policies.

Testing, Monitor and Reporting

38. Primary and Secondary Filtering will be configured to provide automated alerts, reports and logs of potential safeguarding concerns to DSLs. Filtering where possible should reliably identify users and devices to attribute activity and generate timely alerts to DSLs.

39. In-line with KCSIE (2026) paragraph 173, DSLs should carry out an annual review of their approach to online safety, and review filtering and monitoring provision at least annually.

40. Filtering testing will be regularly undertaken by DSL and IT Support Teams and will be tested in partnership with SWGfl and the UK Safer Internet Centre to apply restrictions from the relevant lists – AI-generated content, CSA context, Sexual Content, Terrorist content, etc.

41. Internet traffic monitoring will be regularly undertaken by site IT Teams and reviews of filtering capabilities and categories will be conducted in line with reviews to this policy and government legislation.

42. SNMAT and its Academies have a clearly defined procedure for reporting breaches or failures in filtering. All staff and students will be aware of this procedure by reading the AUP and by receiving the appropriate awareness training.

43. If users discover a website with inappropriate or potentially illegal content, this should be reported to a member of staff who will inform the DSL and the relevant IT Team. All incidents should be documented and, if necessary, reported to appropriate agencies.

44. Although staff will monitor students' use of the internet in lessons, there will be a degree of independence when completing work using the internet.

MICROSOFT 365

WORKSPACE, SHAREPOINT & TEAMS

45. SNMAT promotes the use of Microsoft's 365 and Google Workspace to enhance teaching and learning and to enable learning anywhere via shared resources, email, Classroom, SharePoint and Classroom Team sites. Where possible, no meetings should be held using Zoom, Google Meet or other non-Microsoft platforms.

46. It is the responsibly of any member of staff who is the owner of, or creates a Classroom, SharePoint site, Microsoft Team or shared resource to ensure the correct sharing/access

security is set, to monitor and moderate that resource, and to use the tools available to them to deal with inappropriate behaviour or content.

47. Academies should have Google Workspace and Microsoft Teams and SharePoint policies in place that minimise harm and maximise safety when pupils are using Teams for collaboration or undertaking remote learning.

Storage

48. Microsoft 365 and Google Workspace provides each staff member and students with OneDrive or Google Drive storage mechanisms that can be used to create, access and edit files from any internet-enabled device.

49. Use of Google Drive and OneDrive should be limited to documents such as Word, Excel and Powerpoint, but can store and manipulate images, videos and sound clips under the direction of teaching staff with permission from the Head/Principal. When using Google Workspace and Microsoft 365, staff and students must abide by this policy and all relevant laws regarding the storage and sharing of illegal content.

Other Services

50. To enhance eSafeguarding, some Microsoft 365 services are restricted to students, including the use of Copilot, Webcams, Skype, Chat, Yammer and Kaiza.

REMOVING EVIDENCE FROM DIGITAL DEVICES

51. In accordance with the DfE Searching, Screening and Confiscation in Schools Guidance (2023) and this policy, if a member of staff has grounds to suspect that a digital device contains inappropriate material, or material that has been used in an incident of misuse or breach of eSafeguarding Policy, they will seek consent from the student that the material is removed from the device or in some circumstances shared with the school before it is removed. If the information cannot be shared for technical reasons prior to deletion, then a written description should be taken of the offering material. If staff believe that a law may have been broken, then the phone should be turned off, confiscated and stored securely until police advice is sought.

52. **IMPORTANT: If it is believed that the image/recording is of a sexual nature, it MUST NOT be shared – this is illegal. The device should be turned off, confiscated, stored securely and the issue should be referred immediately to the DSL.**

53. Staff should seek the relevant responsible Pastoral Team or member of SLT to accompany the student to the Academy/School IT Support Team and connect their device to an appropriate secured computer. To mitigate exposure to potential illegal or other inappropriate or private material, the student should locate the required file(s) and move them from the device to a secure location on the school's network.

54. A member of IT Team will remain present to assist if required, and to act as witness.

55. It is the responsibility of the Pastoral Team, or member of SLT to retain an accurate record of evidence that has been taken from digital devices.

ARTIFICAL INTELLIGENCE

56. In line with KCSIE (2026) paragraph 166, schools should follow DfE Using Generative AI in Education and Trust Artificial Intelligence (AI) Guidance to safely and ethically integrate and

manage the use of Artificial Intelligence tools in school.

57. Filtering and Monitoring should be extended to AI tools and AI generated content.

EMERGING TECHNOLOGIES

58. In SNMAT is keen to harness any emerging technologies (such as Virtual Reality, Augmented Reality) that could benefit work practices and teaching and learning. Any new technology will be assessed and evaluated for benefit and security risks before its use is allowed in school.

59. The school will periodically review which technologies which are in use for any security vulnerabilities that may have been discovered since deployment.

60. Prior to deploying any new technologies within the school, staff and students will have appropriate awareness training regarding safe usage and any associated risks.

61. The school will monitor IT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding policy is appropriate.

62. Methods to identify, assess and minimise risks will be reviewed regularly.

REVIEW

63. The application and outcomes of this policy will be monitored to ensure it is working effectively using:

- Logs of reported incidents;
- Monitoring logs of classroom technology and internet activities and filtering;
- Internal monitoring of network activity
- Surveys/questionnaires with pupils/students, parents/carers and staff.

64. This policy is reviewed annually by SNMAT in consultation with recognised trade unions.