FOXWOOD ACADEMY

ONLINE SAFETY AND DIGITAL SAFEGUARDING POLICY

Head Teacher Signature:	J. Hutchinson
Date Adopted:	01.09.2026
Review Date:	01.09.2027

This policy should not be used in isolation. Where an online concern may indicate abuse, neglect, exploitation, child-on-child abuse, harmful sexual behaviour, radicalisation or another safeguarding concern, the Trust Child Protection and Safeguarding Policy takes precedence and the DSL must be informed.

Contents

1. Policy statement and aims

2. Scope

3. Legislation, statutory guidance and related standards

4. Principles and the 4Cs of online risk

5. Roles and responsibilities

6. Online safety education and digital resilience

7. Child-on-child abuse and online harms

8. Sharing nudes and semi-nudes

9. Artificial intelligence and emerging technologies

10. Mobile phones, smart devices and wearable technology

11. Filtering and monitoring

12. Cyber security and information security

13. Acceptable use and professional digital communication

14. Digital images, video and privacy

15. Social media

16. Responding to online safeguarding concerns and incidents

17. Searching, confiscation and electronic devices

18. Parent/carer engagement

19. Training

20. Monitoring, assurance and review

21. Links with other policies

Appendix 1 – Staff quick-reference response

Appendix 2 – Filtering and monitoring annual review

Appendix 3 – AI tool approval/risk assessment

Appendix 4 – Online safety staff self-audit

1. Policy statement and aims

Working and learning online is an essential part of education and of the work undertaken across the Academy and Trust. We recognise the significant educational, social and communication benefits of technology while also recognising that children, staff and other members of the Academy community may experience harm online.

The Academy and Trust will take a safeguarding-first approach to online safety. Online safety is an integral part of safeguarding and child protection rather than a separate technical issue. We will seek to prevent harm, educate children to recognise and manage risk, provide appropriate technical controls, respond promptly to concerns and learn from incidents.

The Trust aims to:

- have robust processes in place to safeguard pupils, staff, volunteers, governors and other members of the Trust community online;
- identify and support pupils who may be at greater risk of online harm, recognising that vulnerability can be affected by age, SEND, EAL, previous experiences of abuse, exploitation, mental health, family circumstances and other contextual factors;
- provide an effective whole-Academy approach to online safety, including mobile and smart technology;
- teach children how to recognise, assess, manage and report online risk and to develop digital resilience;
- ensure that filtering and monitoring are integrated into safeguarding arrangements and are subject to regular review and recorded assurance;
- ensure that staff understand how to respond to online safeguarding concerns and know when an issue must be referred to the DSL;
- ensure that new and emerging technologies, including generative artificial intelligence, are considered through safeguarding, data-protection, curriculum and risk-management processes;
- establish clear mechanisms to identify, intervene, record, escalate and learn from online safeguarding concerns.

2. Scope

This policy applies to all members of the Trust community, including staff, pupils, volunteers, governors, trustees, contractors, agency staff, parents/carers and visitors who use Trust or Academy ICT systems, devices, networks, platforms or online services, whether on or away from Trust premises.

The Academy / Trust may respond to online behaviour that takes place outside Academy where it has a safeguarding, welfare, behaviour, reputational or educational impact on pupils, staff or the wider Academy community. Responses will be proportionate and will follow the relevant safeguarding, behaviour, disciplinary and complaints procedures.

3. Legislation, statutory guidance and related standards

This policy should be read alongside the following statutory guidance, legislation and current standards, as amended from time to time:

- Keeping Children Safe in Education 2026 (KCSIE 2026);
- Working Together to Safeguard Children 2026;
- Education Act 2002 and other relevant education and safeguarding legislation;
- Equality Act 2010;
- Data Protection Act 2018 and UK GDPR;
- Data (Use and Access) Act 2025 and current DfE/ICO data-protection guidance;
- DfE Meeting Digital and Technology Standards in Academys and Colleges – Filtering and Monitoring: Core Standard;
- DfE Meeting Digital and Technology Standards in Academys and Colleges – Cyber Security: Core Standard;

- DfE Mobile Phones in Academys statutory guidance (2026);
- DfE Searching, Screening and Confiscation guidance;
- DfE Teaching Online Safety in Academys guidance;
- DfE Generative AI in Education guidance and Generative AI: Product Safety Standards;
- UKCIS/DfE guidance on sharing nudes and semi-nudes;
- Prevent Duty Guidance and relevant counter-extremism guidance;
- Education for a Connected World and relevant RSHE/relationships and health education requirements;
- Local safeguarding partnership procedures and relevant local authority guidance

4. Principles and the 4Cs of online risk

The Trust's approach is based on the four categories of online risk: Content, Contact, Conduct and Commerce. These categories should be understood as overlapping rather than separate risks.

Content

Being exposed to illegal, inappropriate or harmful content, including pornography, extreme or violent content, racism, misogyny, antisemitism, self-harm and suicide content, extremist or terrorist material, misinformation, disinformation, conspiracy theories and harmful or manipulated AI-generated content.

Contact

Being subjected to harmful online interaction with other users, including grooming, coercion, exploitation, bullying, sexual harassment, abusive behaviour, pressure from peers, adults pretending to be children, and harmful interactions with or through AI systems.

Conduct

Online behaviour that increases the likelihood of or causes harm, including bullying, harassment, misogynistic abuse, harmful sexual behaviour, sharing nudes or semi-nudes, non-consensual sharing of images, impersonation, creation or distribution of deepfakes, and other abusive or criminal behaviour.

Commerce

Risks arising from commercial activity or financial harm, including phishing, scams, fraud, inappropriate advertising, in-app purchasing and other activity that may exploit children or expose them to financial harm.

5. Roles and responsibilities

5.1 Trust Board and governing boards

- provide strategic oversight of online safety and digital safeguarding;
- ensure that online safety is integrated into the wider safeguarding culture and not treated solely as an IT issue;
- ensure that appropriate filtering and monitoring systems are in place and are reviewed at least annually;
- ensure that the annual filtering and monitoring review involves SLT, the DSL, IT support/provider and the responsible governor/trustee, with findings and actions recorded;
- ensure that staff receive appropriate safeguarding and online-safety training and that governors/trustees understand their own responsibilities;
- seek assurance about significant online-safety risks, themes, incidents, training, curriculum provision, AI use, mobile-phone arrangements, filtering/monitoring and cyber security.

5.2 Headteacher and senior leaders

- ensure that this policy is implemented consistently and that staff understand their responsibilities;
- ensure that the Academy has clear arrangements for online safeguarding concerns, including referral to the DSL;
- ensure that staff know how filtering and monitoring operate and how to report concerns about those systems;
- ensure that online safety is reflected in behaviour, safeguarding, curriculum, mobile-phone, acceptable-use and staff conduct arrangements;
- ensure that approved AI tools are subject to appropriate risk assessment and that staff and pupils understand the Trust's expectations for AI use.

5.3 Designated safeguarding lead (DSL) and Deputy DSL (DDSL)

- take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place;
- ensure online safeguarding concerns are managed in line with the Child Protection and Safeguarding Policy;
- work with the headteacher, IT staff/provider and responsible governor to review filtering and monitoring at least annually;
- ensure online-safety risks are considered in safeguarding risk assessment and contextual safeguarding;
- ensure staff receive relevant updates on online harms, AI, child-on-child abuse, sharing nudes/semi-nudes, filtering and monitoring and other emerging risks;
- liaise with children's social care, police, Prevent and other agencies where online harm forms part of a wider safeguarding concern;
- ensure trends and learning from online incidents inform safeguarding practice and curriculum planning.

5.4 Trust IT Director / technical staff

- maintain secure, appropriately configured ICT infrastructure;
- support effective filtering and monitoring and provide the DSL/SLT with relevant information and alerts;
- ensure filtering is active and appropriately applied to managed devices and relevant network access, including devices used away from Academy where applicable;
- support regular testing, maintenance, updates and incident response;
- support the annual filtering and monitoring review and retain technical evidence;
- support cyber-security incident response and report significant incidents through Trust procedures;
- support risk assessment and technical assurance for approved AI products and other emerging technologies.

5.5 All staff, volunteers and contractors

- read and follow this policy and relevant acceptable-use and safeguarding procedures;
- understand how filtering and monitoring work and how to report concerns or suspected failures;
- report online safeguarding concerns promptly to the DSL/deputy DSL and record them on the Academy's safeguarding system where required;
- do not investigate safeguarding concerns themselves or unnecessarily view, copy, forward or redistribute harmful material;
- maintain professional boundaries in all digital communication with pupils and use approved Trust systems;
- use only approved AI tools and comply with Trust data-protection, copyright and safeguarding requirements;
- model respectful, safe and responsible online behaviour.

6. Online safety education and digital resilience

Online safety education forms part of the curriculum and wider safeguarding culture. It will be age-appropriate, developmentally appropriate and adapted where necessary for vulnerable pupils, victims of abuse and pupils with SEND.

Teaching will address both risk avoidance and digital resilience: pupils should be supported to recognise risk, question information, make informed choices, seek help and recover from negative online experiences.

- content, contact, conduct and commerce;
- privacy, personal data, passwords and digital identity;
- online relationships, respectful communication and consent;
- bullying, harassment, sexual harassment and harmful sexual behaviour;
- sharing nudes and semi-nudes and image-based abuse;
- grooming, exploitation and coercion;
- misinformation, disinformation, conspiracy theories and evaluating online sources;
- algorithms, recommendation systems, influencers and commercial content;
- AI-generated content, deepfakes, impersonation and the risks and opportunities of generative AI;
- online scams, phishing, fraud and cyber security;
- radicalisation, extremism and harmful online communities;
- how and where to report concerns, including trusted adults, Academy reporting routes and relevant external services.

7. Child-on-child abuse and online harms

Online harm may be part of child-on-child abuse and must not be treated solely as an ICT or behaviour matter. The Trust will maintain an attitude that abuse can happen here and will respond to online sexual harassment, sexual violence, harmful sexual behaviour, bullying, coercion, misogynistic abuse, image-based abuse, group-chat abuse and other harmful conduct in accordance with the Child Protection and Safeguarding Policy.

Where an online incident suggests that a child may be suffering, or may be at risk of, harm, the DSL will consider the child's wider circumstances and whether multiple or overlapping harms are present. Appropriate early help, safeguarding referral or multi-agency action will be considered.

8. Sharing nudes and semi-nudes

The Trust uses the term 'sharing nudes and semi-nudes' rather than 'sexting'. Incidents involving the making, receiving or sharing of nude or semi-nude images by children are safeguarding concerns and will be managed in line with current DfE/UKCIS guidance and the Child Protection and Safeguarding Policy.

- Staff must not intentionally view, copy, download, forward or otherwise distribute a suspected nude or semi-nude image of a child.
- Where a child discloses that an image exists, staff should listen, reassure and report the concern immediately to the DSL/deputy DSL.
- The DSL will determine the appropriate safeguarding response and whether referral to police, children's social care or another agency is required.
- The Academy will consider the child's welfare, coercion, exploitation, peer pressure, age, vulnerability and the circumstances in which the image was created or shared.
- Staff should preserve relevant contextual information without unnecessarily handling the image itself.

9. Artificial intelligence and emerging technologies

Generative artificial intelligence and other emerging technologies may provide educational benefits but also create safeguarding, privacy, cyber-security, equality, copyright and wellbeing risks. The Trust will take a safeguarding-first and risk-based approach to their use.

9.1 Approved use

- Pupils and staff may only use generative AI products that have been approved through the Trust's agreed process.
- Academies must assess the educational purpose, age appropriateness, safeguarding features, data protection, security, content controls, monitoring and supplier arrangements before approving a product.
- AI products must not be used to make decisions about safeguarding referrals, disciplinary outcomes or other high-impact matters without appropriate human oversight.
- Staff must not enter identifiable pupil information, safeguarding information, special category data or confidential Trust information into an unapproved AI service.

9.2 AI-related safeguarding risks

- AI-generated or manipulated images, audio or video, including deepfakes;
- sexualised or abusive imagery involving children;
- impersonation, bullying, harassment or blackmail;
- AI systems producing harmful, discriminatory, extremist or age-inappropriate content;
- children disclosing personal information or developing inappropriate emotional reliance on AI systems;
- misinformation, disinformation and manipulation;
- AI-assisted scams, phishing or cyber attacks.

9.3 Responding to AI-related incidents

Where a child reports AI-generated or manipulated harmful material involving them or another child, staff must treat this as a safeguarding concern and report it to the DSL in line with the Academy safeguarding policy. Staff must not attempt to investigate by searching for, copying or redistributing harmful sexual or abusive material.

The Trust will keep its AI expectations under review as products, capabilities and national guidance develop.

10. Mobile phones, smart devices and wearable technology

Fom 1 September 2026, academies are expected to operate as mobile-phone-free environments by default. The Trust's arrangements must prohibit pupil access to mobile phones and comparable smart communication devices throughout the Academy day, subject only to agreed exceptions and reasonable adjustments.

- The Academy day includes lessons, movement between lessons, breaktimes and lunchtime.
- The arrangements will be set out in the Academy's behaviour policy and/or a specific mobile-phone policy and communicated clearly to pupils, staff and parents/carers.
- Smart watches and other wearable or connected technologies with comparable communication, recording or notification functionality is included within the Academy's restrictions.
- academies may make reasonable adjustments or other specific arrangements where required because of disability, medical need or other individual circumstances.
- Staff should not use personal mobile phones in front of pupils during the Academy day, except where an appropriate professional reason has been authorised by the headteacher.
- Confiscation and searching will be undertaken in accordance with the behaviour policy and DfE Searching, Screening and Confiscation guidance.

- Residential trips, off-site activities and arrangements outside the normal Academy day will be managed through the relevant Academy/trip risk assessment and policy.

11. Filtering and monitoring

Filtering and monitoring are safeguarding controls and must not be regarded as solely technical functions. The Trust will ensure that provision reflects the Academy's age profile, pupil risk profile, SEND/EAL considerations, technology use and emerging risks including AI-generated content.

11.1 Roles and assurance

- The Trust board has overall strategic responsibility.
- A named member of SLT will have operational responsibility for filtering and monitoring – Mr J Hutchinson
- The DSL will take lead responsibility for understanding filtering and monitoring from a safeguarding perspective – Mr J Hutchinson
- The Trust IT team/technical provider will manage the technical configuration, maintenance and technical response.
- A responsible governor/trustee will receive assurance through the annual review – Foxwood Safeguarding governor

11.2 Annual review

- Filtering and monitoring will be reviewed at least once every academic year and sooner where significant changes occur.
- The review will involve SLT, the DSL, IT support/provider and the responsible governor/trustee.
- The review will identify current provision, gaps, limitations, pupil risk factors, coverage, monitoring alerts and required actions.
- The Trust will record who undertook the review, when it took place, what was checked, findings, actions, owners and completion dates.
- The review will consider managed devices, relevant unmanaged/BYOD devices where applicable, guest access and devices used away from Academy.
- Monitoring arrangements will include a documented process for responding to alerts, including immediate escalation of high-risk safeguarding or technical incidents.

11.3 Exceptions and failures

Temporary exceptions to filtering or monitoring must be authorised and documented by the appropriate SLT lead. Where filtering or monitoring is unavailable or known to be ineffective, the Academy will implement alternative risk controls and report the issue through Trust procedures.

12. Cyber security and information security

Online safeguarding depends on secure systems. The Trust will maintain appropriate cyber-security controls and will manage cyber incidents through the Trust's Cyber Security Policy and incident-response procedures.

- Staff must use approved accounts, devices and authentication arrangements.
- Passwords/passphrases and multi-factor authentication must comply with Trust technical requirements.
- Devices and software must be kept appropriately updated and protected.
- Lost or stolen devices, compromised accounts, suspected phishing, malware or other security incidents must be reported promptly to the Trust IT team.

- Safeguarding and personal data must be handled in accordance with the Trust Data Protection Policy and relevant legal requirements.
- Cyber-security risks arising from third-party suppliers, apps and AI products must be considered before adoption.

13. Acceptable use and professional digital communication

All pupils, parents/carers, staff, volunteers, governors, trustees and relevant visitors must comply with the Trust/Academy Acceptable Use Agreement applicable to them.

- Digital communications between staff and pupils/parents must be professional in tone and content and use approved Trust systems.
- Personal email addresses, personal messaging accounts and public social-media messaging must not be used for direct professional communication with pupils.
- Users should assume that activity on Trust systems may be monitored in accordance with law and the Trust's policies.
- Users must report content or communications that are threatening, abusive, discriminatory, sexually inappropriate or otherwise concerning.
- Staff must respect copyright, licensing and intellectual property requirements.
- Use of AI must comply with the Trust's approved-AI process and data-protection requirements.

14. Digital images, video and privacy

Digital images and video can support learning and communication but create privacy and safeguarding risks. Staff must follow the Trust's image, data-protection and communications procedures.

- Staff should use Trust/Academy equipment and approved storage systems for Academy photography and video wherever practicable.
- Images must be collected, stored, shared and published in accordance with the Trust's privacy notices and image-consent arrangements.
- Care must be taken to avoid unnecessary identification of pupils and to ensure that images are appropriate and dignified.
- Pupils must be taught about consent, privacy, image sharing, permanence and the risks of redistribution.
- Staff must not use personal devices to store pupil images unless explicitly authorised under Trust procedures.

15. Social media

Official Academy and Trust social-media accounts may be used for communication and community engagement only where approved. Staff must maintain professional boundaries and comply with the Staff Code of Conduct.

- Staff must not establish informal social-media groups with pupils using personal accounts.
- Any educational online community or platform must be approved and appropriately moderated.
- academies should consider safeguarding, privacy, moderation, accessibility and data-protection risks before introducing a new online platform.
- Concerns about fake accounts, impersonation, harassment or inappropriate contact involving a pupil or member of staff should be reported through the relevant safeguarding or conduct procedure.

16. Responding to online safeguarding concerns and incidents

All online safeguarding concerns will be managed in line with the Trust Safeguarding Policy. The online element must not delay a safeguarding response.

16.1 Staff response

- Listen and take the concern seriously.
- Reassure the child that they have done the right thing by telling an adult.
- Do not investigate the concern yourself.
- Do not unnecessarily view, copy, forward or redistribute harmful content.
- Report the concern immediately to the DSL/deputy DSL.
- Record the concern on the Academy's safeguarding recording system in accordance with local procedures.
- Follow any direction from the DSL about preservation of relevant evidence and contact with parents/carers or external agencies.

16.2 Escalation

The DSL will consider whether the incident indicates abuse, neglect, exploitation, child-on-child abuse, harmful sexual behaviour, radicalisation, a criminal offence, a data-protection breach or another safeguarding concern. Appropriate referral or multi-agency action will be taken where required.

16.3 Learning

Significant incidents and emerging themes will be reviewed by SLT and the DSL and, where appropriate, reported to governors/trustees. Learning should inform curriculum content, staff training, technical controls and policy review.

17. Searching, confiscation and electronic devices

Searching, screening and confiscation will be carried out in accordance with current DfE guidance, the Academy's behaviour policy and the law.

- Staff must have appropriate authority and reasonable grounds in accordance with the relevant policy before searching.
- Searches must be proportionate and take account of the pupil's age, SEND and individual circumstances.
- Where a device may contain evidence of a safeguarding concern or offence, staff should seek advice from the DSL and follow the relevant safeguarding/police procedures.
- Where staff suspect that a device contains a nude or semi-nude image of a child, they must not intentionally view the image and must refer immediately to the DSL.
- Staff must not delete potentially evidential material where it may be relevant to a suspected offence; advice should be sought from the DSL/police as appropriate.

18. Parent/carer engagement

Parents and carers play a crucial role in helping children understand online risk. The Trust will provide accessible information and opportunities for parents/carers to understand current risks and the Academy's arrangements.

- how filtering and monitoring operate;
- mobile-phone and smart-device expectations;
- AI and emerging technology risks;
- social media, gaming and age-appropriate digital communication;
- sharing nudes/semi-nudes and image-based abuse;

- online bullying, harassment and harmful content;
- how to report concerns to Academy and where to seek further help.

19. Training

Online safety forms part of safeguarding training and induction. All staff will receive relevant training at least annually, together with updates where risks, technology, guidance or Trust arrangements change.

Training will include, as appropriate:

- the 4Cs and current online harms;
- child-on-child abuse and harmful sexual behaviour online;
- sharing nudes/semi-nudes;
- AI, deepfakes and emerging technologies;
- filtering and monitoring responsibilities and incident response;
- mobile-phone and smart-device expectations;
- cyber security and data protection;
- radicalisation and extremist content online;
- how to respond to and record an online safeguarding concern.

DSLs and deputy DSLs will undertake safeguarding training in accordance with the Trust Safeguarding Policy and will maintain current knowledge of online safety and filtering/monitoring.

20. Monitoring, assurance and review

The Trust will review this policy at least annually and sooner where there is a significant change in legislation, statutory guidance, technology, safeguarding risk, Trust practice or following a significant incident.

- The DSL will lead the Academy's annual review of online safety, working with SLT and IT staff.
- The review will consider curriculum, staff training, parental engagement, incidents, vulnerable groups, AI use, mobile devices, filtering and monitoring, cyber security and emerging risks.
- The filtering and monitoring annual review will be recorded separately and reported through governance arrangements.
- Significant findings and actions will be reported to the governing board/trustees.
- The Trust will use incidents and emerging trends to improve practice rather than relying solely on compliance checks.

21. Links with other policies

- Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Low-Level Concerns / Managing Allegations Policy
- Data Protection Policy and Privacy Notices
- Cyber Security Policy
- ICT / Acceptable Use Policy
- Mobile Phone Policy or relevant Behaviour Policy section
- Prevent and counter-extremism procedures
- Complaints Procedure

- Equality Policy
- SEND policy and reasonable-adjustment arrangements
- Educational Visits / Residential Visits policies

Appendix 1 – Staff quick-reference: responding to an online safeguarding concern

1. LISTEN

Take the concern seriously. Listen without judgement and reassure the child.

2. DON'T INVESTIGATE

Do not search for, copy, forward or unnecessarily view harmful content. Do not question other pupils to establish the facts.

3. REPORT

Tell the DSL/deputy DSL immediately if the concern may indicate harm. The Headteacher at Foxwood is the designated ESafety lead.

4. RECORD

Make an accurate safeguarding record in accordance with the Academy's recording system.

5. FOLLOW THE DSL

The DSL decides on safeguarding action, parent/carer contact, external referral and evidence preservation.

6. LEARN

Where appropriate, incidents inform curriculum, training, technical controls and policy review.

Appendix 2 – Filtering and monitoring annual review

Date - **September 2026**	J. Hutchison, Alice Poppleton, Matt Robertson, Lindsey Norton

This checklist is intended to evidence the annual review required by the DfE Filtering and Monitoring: Core Standard.

Review area	Evidence / finding	Action / owner	Completion date
Named SLT lead and responsible governor/trustee identified	Yes	J.Hutchinson - Headteacher. Safeguarding governor	9/26
DSL understands filtering and monitoring arrangements	Trust have central control of filtering and monitoring. Foxwood have additional 'Securus Software' that emails immediate alerts. AP/JH/LN check every 48 hours to review screenshots arranged by severity	J. Hutchinson	9/26
IT/provider responsibilities confirmed	TBC -	Trust IT	TBC
Filtering coverage checked across managed devices and relevant networks	In place	Trust IT	
BYOD/guest access considered where applicable	Policy	Policy	Jan 2027
Monitoring reports reviewed, including high-risk alerts	Review by A. Poppleton (Monday) L. Norton (Wednesday) J. Hutchinson (riday) Emails sent by system for higher severity. High risk concerns recorded on safeguarding system	J. Hutchinson/A. Poppleton	9/26
High-risk incident escalation process tested	Yes	J. Hutchinson	9/26
Safe-search / filtering categories reviewed	Trust	Trust IT	Ongoing Sep 26
AI-generated and dynamic content risks considered	Yes, training in September A. Poppleton	A.Poppleton	9/26

Pupil risk profile, SEND and EAL considered	Yes – Profiles on Prvision Map, vulnerability matrix scores children	S.Porter	9/26 (VM scores updated in November each year)
Temporary exceptions reviewed and documented	Yes	In partnership with Trust IT when needed	9/26
Technical limitations/gaps identified	Yes, filtering is the first safety net, then the Securus emails, then the 48 hour check - there may always be a chance that online information/checks are not filtered. The final net of course is that children and young people are very rarely unsupervised at Foxwood	J. Hutchinson	
Staff awareness of reporting processes checked	Yes – quiz to be sent out in January as an update, regular National College Training recorded internally	J. Hutchinson/ A.Poppleton	9/26 01/27
Actions from previous review completed or carried forward	N/A		
Findings reported to governors/trustees	TBC		

Appendix 3 – AI tool approval / risk assessment

No new AI tool should be introduced for pupil or staff use without completion of the Trust's agreed approval process. The following headings should form part of that process.

Product/tool and supplier:	
Educational purpose:	
Age suitability:	
Safeguarding/content controls:	
Filtering and monitoring capability:	
Data collected and processing:	
Where data is stored:	
Account requirements and authentication:	
AI-generated content risks:	
Emotional/social/mental-health considerations:	
Cyber-security considerations:	
Copyright/intellectual-property considerations:	
Accessibility/SEND considerations:	
Parental communication required:	
Human oversight and staff supervision:	
Decision: Approved / Approved with conditions / Not approved	
Review date:	

Appendix 4 – Online safety staff self-audit

Question	Yes / No	Action / training need
Do you know who has lead responsibility for online safety and safeguarding in your Academy?		
Do you know how to report an online safeguarding concern?		
Do you understand the Academy's filtering and monitoring arrangements?		
Do you know how to report a filtering or monitoring failure?		
Do you know what to do if a child shows you a harmful image or message?		
Do you know the Academy's arrangements for sharing nudes/semi-nudes?		
Do you understand the Trust's expectations for AI use?		
Do you know which AI tools are approved?		
Do you understand the Academy's mobile-phone and smart-device arrangements?		
Are you aware of current online child-on-child abuse risks?		
Are you aware of online radicalisation and extremist-content risks?		
Do you understand the cyber-security and data-protection requirements that apply to your role?		
Do you know where to find the Acceptable Use Agreement and related policies?		
Do you know what to do if an online incident suggests a child may be at risk of harm?		