GREENWOOD ACADEMIES TRUST

Trust Online Safety Policy

Document Owner:	Deputy Chief Executive Officer
Version	2
Effective From:	January 2026

Background

Awareness of online safeguarding risks is essential for both young people and staff. With the increasing use of digital technologies, pupils are exposed to various harmful and inappropriate online material such as cyberbullying, online grooming, and exposure to inappropriate content.

By being aware of these risks, pupils can take proactive measures to protect themselves and their peers. This awareness also empowers them to report any suspicious or harmful activities to trusted adults, ensuring a safer online environment for everyone. For staff, understanding these risks is essential to effectively monitor and guide pupils' online activities, ensuring that they adhere to safe practices and avoid potential dangers, as well as keeping themselves safe online.

This policy provides a structured approach to managing these risks through a set of technical measures and cultural awareness and provides a consistent and comprehensive framework for online safety, fostering a culture of vigilance and responsibility among both pupils and staff. This not only helps in mitigating risks but also promotes a positive and secure digital learning environment.

General Online Safeguarding Risks

General digital safeguarding risks are dynamic and will be kept under review. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; for example: 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: 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,

and Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Significant risks include:

- **Access to inappropriate content**
- **Bias and discrimination**
- **Cyberbullying**: Ensuring that pupils are protected from cyberbullying and have the resources to report and address it
- **Deepfakes**
- **Harmful targeted websites and adverts**
- **Online abuse**
- **Online grooming**

- **Online predators**
- **Sextortion**

Relevant Guidance

This policy complies with relevant requirements of the Department of Education's Keeping Children Safe in Education, Digital and Technology Standards in Schools and Colleges and Generative AI: Product Expectations and DFE Generative AI in Education.

Generative AI

GAT's AI Protocol sets out the conditions for the safe use of AI and should be read in conjunction with this policy.

GAT is particularly aware of the potential to use Generative AI to provide additional insight, which will help it personalise pupil learning and support. This increased ability to gain greater insight also comes with potential additional risks, which must be fully considered in developing the insight.

GAT will support pupils general understanding of the risks of using generative AI through the delivery of the PSHE curriculum.

The use of Generative AI should only be used where the benefits of use outweigh the risks of using in and in the best interest of the pupil.

Roles and Responsibilities

The following section outlines roles and responsibilities. The Trust recognises that all members of the community have important roles and responsibilities to play with regard to online safety:

The Trust Board

The Trust Board is responsible for monitoring the overall effectiveness of our approach. The Board will receive regular information about online safety issues via the relevant committee to ensure that they are doing all they reasonably can to limit online safety risks. This will include review of Trust filtering and monitoring systems.

The Executive Leadership Team (ELT)

ELT are responsible for ensuring effective implementation and review of this policy. ELT will ensure that the Trust Board receive regular information about online safety issues via the relevant committee. ELT will set expectations regarding Trust Quality Assurance and will ensure regular review of this policy and that their directorate teams are aware of the policy.

Technology, and risks and harms related to it, evolve, and change rapidly. The Trust will carry out a review at least annually, of its approach to online safety, supported by an annual risk assessment that considers and reflects the risks.

Principals

The Principal will be accountable for the following, although they may delegate day-to-day leadership responsibilities to other members of the academy leadership team;

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with Trust expectations as described in this policy and national recommendations and requirements;
- ensure the academy follows Trust policies and practices regarding online safety, information security and data protection:
- ensure that pupils are aware of their own responsibilities under this policy and ensure that parents and carers are aware of aspects of this policy that apply to them
- ensure that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety;
- support the DSL and Online Safety Lead by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities in relation to online safety and filtering and monitoring systems;
- ensure that all staff complete regular, up to date and appropriate online safety training;
- be aware of what to do in the event of a serious online safety incident, and ensure the use of Trust reporting channels for online safety concerns;
- receive regular reports from the DSL on online safety to ensure appropriate action is being taken in their academy.

Designated Safeguarding Leads (DSLs)

DSLs take day to day responsibility for the online safety of pupils and have responsibility for;

- understanding the filtering and monitoring systems in place;
- promote an awareness of and commitment to online safety throughout the academy community and ensure all staff are aware of their responsibilities regarding filtering and monitoring systems;
- ensure there is an identified Online Safety Lead who facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the academy community, as appropriate;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- respond in a timely way to reported concerns regarding pupil internet usage, taking relevant action where required.

Online Safety Lead (OSLs)

Each academy has a named OSL's who will work with the DSL to review the academy online safety approach. They are also responsible for:

- ensuring they keep up to date with national, local and Trust updates regarding online safety
- facilitate training and advice for all staff keeping colleagues informed of current research, legislation and trends regarding online safety;
- have knowledge and understanding of the Trust filtering and monitoring systems, Gen AI and cyber security systems and communicating this to the academy community;

- act as the named point of contact on all online safety issues, and liaise with other members of staff or other agencies;
- keep the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils.

Staff

All staff will;

- read and adhere to this policy in relation to online safety;
- take responsibility for their own appropriate use of Trust/academy systems and the data they use, or have access to;
- model safe, responsible and professional behaviours in their own use of technology;
- have an up to date awareness of a range of online safety issues and how they may be experienced by pupils through ensuring their training and knowledge is up to date;
- know when and how to escalate online safety issues.

Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities)

Pupils will :

- have an up to date awareness of a range of online safety issues and how they may be experienced by pupils through the Academy curriculum offer; read and adhere to relevant academy online safety documents;
- take responsibility for keeping themselves safe online;
- and report to a trusted adult, if there is a concern online.

Parents and carers:

We believe that our work in the area of online safety will be greatly enhanced if we have the engagement and support of all our parents and carers, it is therefore recommended that they are aware of the importance of:

- encouraging their children to adhere to academy online safety documents; supporting the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home;
- modelling safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children;
- understanding changes in behaviour could indicate that their child is at risk of harm online;
- seeking help and support from their child's individual academy, or other appropriate agencies, if they or their child encounter risk or concerns online;
- using school systems, such as learning platforms, and other network resources, safely and appropriately; and taking responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

IT Managed Service Partner (MSP)

The MSP will manage the technical IT environment to ensure the safety and security of GAT's key enterprise level systems based on Microsoft technologies, which provide expertise and advice in relation to prevailing online safety risks, in line with Microsoft security guidelines.

Cyber Security Partner

GAT's Cyber Security Partner provide further expertise, support, intelligence and monitoring (Security Operations Centre) to GAT to ensure that is can manage its Cyber Security risks.

External groups and organisations

External groups and organisations will be expected to read, understand and implement all relevant online safety documentation and expectations prior to being given individual access to any Trust network and ensure they adhere to these at all times as specified in our Bring Your Own Device Policy.

Filtering

In order to protect pupils from accessing harmful online content and staff accessing inappropriate content, GAT applies filtering and monitoring polices which apply to all GAT owned student and staff devices.

GAT will work with its IT MSP to determine a list of blacklisted search categories, which will be kept under regular review and maintained by our MSP and Safeguarding Directorate.

Any request to whitelist a website within a blacklisted category will be made to the MSP IT Service Desk, and if the request is considered not to lead to an unacceptable risk by the MSP and GAT' s Safeguarding Directorate, approval will be sought from the academy principal. A register of approved requests will be maintained by the MSP on behalf of GAT.

Monitoring

Online activity of all staff and pupils across the Trust is monitored by the Safeguarding Directorate via the Trust Internet monitoring system maintained by GAT's MSP.

DSLs within academies are informed of incidents of pupil misuse/potential risk as reported via the Online Filtering System. Any incidents of this type should be dealt with through normal behaviour and disciplinary procedures with consideration given to safeguarding concerns in every incident.

Identified concerns relating to the online activity of Trust staff will be followed up through the relevant Directorate.

If you witness/become aware of any online safety issues you must refer this to the Academy DSL or your line manager.

GAT uses Microsoft Copilot Chat and M365 as its preferred Generative AI LLM, which operates under Microsoft's ethical AI framework. GAT has access to all staff prompts made in Microsoft Copilot and may review any prompts failing Microsoft's ethical AI filtering.

Cyber Security and Data Privacy

GAT takes its responsibilities to ensure that pupils and staff data is private and secure and that access to online data, systems and software can be achieved whilst ensuring the protection of personal data. GAT operates a Zero Trust Cyber Security Policy and utilises cyber security experts to support the delivery of that policy.

As a part of an extensive approach to managing the risk of cyber security, GAT has received the Cyber Essentials Plus accreditation.

Online Safety Awareness and Training

Pupils will develop online safety skills through their curriculum, including through the delivery of PSHE. Staff will receive regular safety cyber security training and phishing exercises.

Specific Technology Issues

Online meetings

Only Microsoft Teams will be used for any GAT organised online meeting. For the avoidance of doubt, GAT will only utilise any other meeting platforms, including Zoom, Google Meet up, etc if these platforms are insisted on by other external agencies who have arranged the meeting.

All participants in any online meeting organised by GAT (including online learning) will be expected to have their cameras on to ensure that all participants are those expected.

The only meeting notetaking or transcription application that will be used by GAT will be through Microsoft Office.

Education Software

Any educational software used by pupils or staff, accessed on a GAT device must go through GAT's Software Screening Protocol administered within its software protocol.