ONLINE SAFETY POLICY

The Thomas Alleyne Academy

DOCUMENT PRODUCED BY:	KATE PRINCE (BUSINESS MANAGER) DEVON WOOLLEY (DSL)
DATE APPROVED:	September 2024
NEXT REVIEW DATE:	July 2026

1. INTRODUCTION

The Thomas Alleyne Academy recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast-moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** students, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. LEGAL FRAMEWORK

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

3. RESPONSIBILITIES

The head teacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is the DSL who coordinates online safety at the Academy, and all breaches of this policy must be reported to him
All breaches of this policy that may have put a child at risk must also be reported to a Designated Senior Person in person and/or via CPOMS.

Staff, governors and students should not open emails or attachments from suspect sources and should report their receipt to the ICT Manager.

Student specific:

- Adhere to the Acceptable Use Agreement and other relevant policies
- Seek help from school staff if they are concerned about something they or a peer have experienced online.
- Report online safety incidents and concerns in line with the procedures within this policy.

Staff and Governor specific:

- Adhere to the Acceptable Use Agreement and other relevant policies
- Take responsibility for the security of ICT systems and electronic data they use or have access to.
- Model good online behaviours.
- Maintain a professional level of conduct in their personal use of technology.
- Have an awareness of online safety issues.
- Ensure they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Report concerns in line with the school's reporting procedure.
- Where relevant to their role, ensure online safety is embedded in their teaching of the curriculum.

Separate organisations that are renting space from the school should have, and follow, their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of students is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

4. SCOPE OF POLICY

The policy applies to:

- students
- parents/carers
- teaching and support staff (including staff who have accepted a position at the Academy, and are using online resources in preparation for their employment start date)
- academy governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the Academy's facilities

The Academy also works with partners and other providers to ensure that students who receive part of their education off site or who are on an Academy trip or residential are safe online.

The Academy provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

5. POLICY AND PROCEDURE

The Academy seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The Academy expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on

appropriate online behaviour and use of technology outside of the Academy for students, parents/carers, staff and governors and all other visitors to the Academy.

Use of email

Staff and governors should adhere to the ICT User Agreement. Staff must use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students or parents or conduct any Academy business using a personal email address.

Students in year 7-11 will not have access to a school email account. Year 12 and 13 will have access to email and will adhere to the Sixth Form ICT Agreement. They will use school approved accounts on the school system for educational purposes. Where required, parents/carer permission will be obtained for the student account to exist.

For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection policy. Emails created or received as part of any Academy role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in Academy or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with Mrs J Cooke, or the Hart Learning Group Data Protection Officer in her absence, with details of the site/service. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content. When working with students, searching for images should be done through Google Safe Search (standard through the HfL Broadband service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
    - Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
    - Adult material that breaches the Obscene Publications Act in the UK
    - Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the Academy or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the Academy

- Use the Academy 's hardware and/or Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the Academy

All instances of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The Academy recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Head of Department or Senior Leader responsible for that department.

Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the Academy. In line with GDPR they are used only with the written consent of parents/carers, which is secured in the first instance on a child's entry to the Academy. Records are kept on Arbor, and consent can be changed by parents/carers at any time. (See Data Protection policy for greater clarification).

Photographs and images of students are only stored on the Academy's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted, as appropriate to the purpose and audience – e.g, ID, celebration of achievement etc. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the Academy's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the Academy community, other than their own child/ren.

Staff, and other professionals working with students, must only use Academy-approved equipment to record images of students whether on or off site.

Use of personal mobile devices (including phones)

Parents/carers should refrain from using personal mobile phones in the presence of children whilst on the Academy premises. If a visitor, parent or carer is seen using their mobile phone, they will be asked politely to turn it off and remove it from children's view. At times images be taken on Academy premises or on off-site Academy events and activities, e.g. Sports Day, but it will be made clear in advance when this is applicable .

Students are allowed to bring personal mobile devices/phones to the Academy but must not use them for personal purposes whilst on school site. All such devices must be switched off/silent whilst on school site.

Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The Academy is not responsible for the loss, damage or theft on Academy premises of any personal mobile device.

Users bringing personal devices into the Academy must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the Academy must consider the educational benefits, and carry out risk assessment before use on-site is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in the Academy and should check before they are brought on-site.

Reporting incidents, abuse and inappropriate material

There may be occasions when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL, the head teacher or deputy DSL. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The Academy takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

6. CURRICULUM

Online safety is fully embedded within our curriculum. The Academy provides a comprehensive age appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, academy details, IM/email address) and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

7. STAFF AND GOVERNOR TRAINING

Staff and governors are trained to fulfil their roles in online safety. The Academy audits the training needs of all Academy staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the Academy's Acceptable Use Agreement as part of their induction and before having contact with students.

~~Any organisation working with children based on the Academy premises is required to sign the Acceptable Use Agreement. This agreement is available in the Staff Shared Area and reviewed annually.~~

~~Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement.~~

In some circumstances, it is necessary to provide access to people working at school with a guest login, which provides access to a singular drive (not network) and internet access. Visitors using the guest login must sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and parent/carer helpers in the form of a leaflet which is also available online via a link on the academy website.

8. WORKING IN PARTNERSHIP WITH PARENTS AND CARERS

The Academy works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.
It is important that parents/carers understand the crucial role they play in this process. The Academy seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The Academy provides regular updated online safety information through the Academy website and by other means.

Parents and carers are reminded via communications and fortnightly newsletter about the acceptable use of internet connected devices in school and this is discussed with individuals at parent meetings as appropriate, A summary of key parent/carer responsibilities will also be provided and is available on the academy website. The Acceptable Use Agreement explains the Academy's expectations and student and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

9. RECORDS, MONITORING AND REVIEW

The Academy recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Safeguarding concerns must be logged on CPOMS.

The Academy supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the Academy's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy every three years.

10. FILTERING AND MONITORING ONLINE ACTIVITY

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The business manager and ICT staff will determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT staff will undertake monthly checks on the filtering and monitoring systems, including use of the South West Grid for Learning's (SWGfL) testing tool to check that school filtering system is effective and appropriate.

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

Requests regarding making changes to the filtering system will be directed to the ICT staff and approved by the DSL. Prior to making any changes to the filtering system, ICT staff and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT staff. Reports of inappropriate websites or materials will be made to an ICT staff member immediately, who will work with the HfL Education technical team or DSL (as appropriate) to investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT staff, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

11. REVIEW

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.
The governing board, business manager,headteacher and DSL will review this policy in full every two years and following any online safety incidents.

12. RELATED POLICIES/ DOCUMENTS

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole academy community.

Academy Policies

- Anti-Bullying Policy
- Bring Your Own Device Policy
- Behaviour Policy
- Cyber Security
- Visitors Policy and Procedures
- Child Protection
- Remote Learning Policy

Group Policies

- Staff Code of Conduct Policy
- Data Protection
- E Safety & Data Security