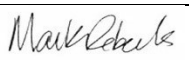
PENK VALLEY
ACADEMY TRUST

On Line Safety Policy

Adopted by Trustees:	
Signed:	
Date:	**Autumn 2026**
This policy is reviewed annually by the Finance, Audit and Risk Committee.	
Next Review date:	**Autumn 2027**

POLICY INFORMATION

Date of last review:	Autumn 2026	**Review period:**	Annually
Date ratified by Trustees:	Autumn 2026	**Trustee committee responsible:**	Finance, Audit and Risk
Policy owner:	Chief Operations Officer	**Executive team member responsible:**	Chief Operations Officer

Reviews/revisions

Review date	Changes made	By whom
2017	Policy introduced	Trust officers
2018	Schools added and policy amended for PVAT	Trust officers
2020	Technical and organisational updates	Trust officers
2021	Filtering and monitoring updates	Trust officers
2022	Monitoring system and roles updated	Trust officers
2024	Operational updates	Trust officers
2025	Annual update	
Autumn 2026	Full rewrite focused on online safety, with safeguarding procedures cross-referenced to the adopted safeguarding policy; strengthened provisions on annual risk assessment, cyber security education, AI-enabled harms, device searching, visitors and incident recording	Chief Operations Officer

Equality and GDPR

All Penk Valley Academy Trust policies should be read in conjunction with our Equal Opportunities and GDPR policies.

Statement of principle – Equality

We will take all possible steps to ensure that this policy does not discriminate, either directly or indirectly against any individual or group of individuals. When compiling, monitoring and reviewing the policy we will consider the likely impact on the promotion of all aspects of equality as described in the Equality Act 2010.

Statement of principle – GDPR

Penk Valley Academy Trust recognises the serious issues that can occur as a consequence in failing to protect an individual adult's or child's personal and sensitive data. These include emotional distress, physical safety, child protection, loss of assets, fraud and other criminal acts.

Penk Valley Academy Trust is therefore committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA)/GDPR.

Penk Valley Academy Trust will be referred to as **PVAT** for the remainder of the document which includes all schools who are members of PVAT, business operations and centralised services.

ONLINE SAFETY POLICY

Penk Valley Academy Trust will be referred to as PVAT throughout this policy. The term school includes every academy within PVAT, together with central services and Trust-wide operations.

Contents

Equality and GDPR 2

1. Purpose and scope 3

2. Relationship with safeguarding and other policies 4

3. Online safety risks 4

4. Roles and responsibilities 4

4.1 Trustees and executive leadership 4

4.2 Headteachers and Designated Safeguarding Leads 5

4.3 Trust ICT function and technical support 5

4.4 Staff and other adults 5

4.5 Pupils, parents and carers 5

5. Online safety education 5

6. Filtering and monitoring 6

7. Safe and appropriate use of technology 6

8. Communication, social media, images and recordings 6

9. Responding to online safety concerns 7

10. Parents, carers and the wider community 7

11. Training, monitoring and review 7

1. Purpose and scope

PVAT recognises that technology is integral to education, communication and school operations. This policy sets out the Trust's arrangements for helping pupils and adults use technology safely, responsibly and respectfully, for reducing exposure to harmful online content and activity, and for maintaining appropriate filtering and monitoring arrangements.

The policy applies to trustees, employees, agency staff, contractors, volunteers, pupils, parents and carers, visitors and community users when using Trust systems or taking part in Trust-related online activity. It applies to Trust-owned and personal devices where they are used on Trust premises, connected to Trust networks, used for Trust business or involved in an incident affecting the school community.

It covers internet access, email, messaging, learning platforms, cloud services, social media, video conferencing, online games and communities, mobile and wearable devices, photography and recording, artificial intelligence services and other current or emerging digital technologies.

2. Relationship with safeguarding and other policies

Online safety is an aspect of safeguarding, but this policy does not restate the Trust's child protection procedures. Each school follows the safeguarding policy adopted from the local authority model, which sets out how concerns about a child, allegations or concerns about adults, child-on-child abuse, referrals, escalation and liaison with the Local Authority Designated Officer and other agencies must be managed. Where online activity gives rise to a safeguarding concern, that policy and the school's established safeguarding procedures take precedence.

This policy should also be read alongside the Cyber Security and ICT Acceptable Use Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Generative Artificial Intelligence Policy and any school-specific rules for mobile devices. Personal data is handled in accordance with the General Data Protection Regulation Policy, the Appropriate Policy Document for special category and criminal offence data and the relevant privacy notices. The data protection policies and privacy notices are available on the Penk Valley Academy Trust website.

3. Online safety risks

PVAT uses the four areas of online risk described as content, contact, conduct and commerce. The categories overlap and should be considered in the context of the pupil's age, needs and circumstances and the nature, frequency and impact of the activity.

Area	Description
Content	Exposure to illegal, inappropriate or harmful material, including discriminatory content, violent material, misinformation, harmful challenges, self-harm content and age-inappropriate material.
Contact	Harmful interaction with other users or AI-enabled services, including bullying, pressure, grooming, coercion, exploitation, impersonation, unwanted contact, manipulative interactions and false or simulated relationships.
Conduct	Online behaviour that causes or increases harm, including abusive communication, unsafe sharing, image-based abuse, sextortion, inappropriate disclosure of personal information, infringement of privacy, the creation or distribution of deepfakes or AI-generated imagery, and attempts to evade school controls.
Commerce	Risks arising from advertising, scams, phishing, in-app purchasing, gambling-like features, financial exploitation and other persuasive or fraudulent design.

Online activity may be connected with bullying, exploitation, radicalisation, harmful behaviour between pupils or other safeguarding concerns. The purpose of this policy is to identify and reduce the online element of those risks. The assessment and management of any resulting safeguarding concern is governed by the safeguarding policy. Online bullying, harassment and intimidation, including activity through social media, messaging platforms, gaming environments and emerging technologies, will be managed in accordance with the Behaviour Policy and Anti-Bullying Policy.

4. Roles and responsibilities

4.1 Trustees and executive leadership

The Board of Trustees has strategic responsibility for ensuring that appropriate online safety arrangements are in place. Trustees will receive assurance about online safety education, filtering and monitoring, staff awareness and material themes or control weaknesses. The Chief

Executive Officer retains overall executive accountability, supported by the Chief Operations Officer as policy owner.

4.2 Headteachers and Designated Safeguarding Leads

Each Headteacher is responsible for implementing this policy within their school, ensuring that staff understand the arrangements and that pupils receive appropriate online safety education. The Designated Safeguarding Lead will understand the filtering and monitoring provision, contribute to its review and ensure that online concerns with a safeguarding dimension are managed through the school's safeguarding procedures.

4.3 Trust ICT function and technical support

The Trust ICT function and contracted technical providers will implement and maintain approved filtering and monitoring controls, manage authorised access and provide information needed for review and assurance. Technical staff will pass safeguarding-related alerts or concerns to the appropriate school role and will not make safeguarding decisions in isolation.

4.4 Staff and other adults

Staff, contractors and volunteers must model safe and professional use of technology, comply with acceptable use requirements, use authorised systems, protect account credentials and report concerns promptly. They must maintain professional boundaries in online communication and seek approval before introducing new digital services for Trust use.

Visitors and community users who access Trust systems or networks must comply with applicable acceptable use requirements and any conditions of access provided by the school.

4.5 Pupils, parents and carers

Pupils are expected to use technology safely, responsibly and respectfully, follow age-appropriate acceptable use expectations and report anything that worries them. Parents and carers are encouraged to reinforce safe use at home, discuss online activity with their child and raise concerns with the school. Current role-holders and contact routes will be communicated through school information rather than personal names being included in this policy.

5. Online safety education

Online safety will be taught through an age-appropriate, progressive curriculum and reinforced through everyday use of technology, assemblies, pastoral work and relevant subjects. Teaching will help pupils evaluate information, manage privacy and digital identity, communicate respectfully, recognise manipulation and harmful contact, protect accounts and devices, understand the possible audience and permanence of online material, check the reliability of information and respect copyright and intellectual property. Pupils will also be taught age-appropriate cyber security skills, including secure password practices, phishing and social engineering awareness, authentication methods, physical device security, safe use of removable storage, protection of personal information and how to report a cyber incident or personal data breach.

Education will reflect the age, development, needs and vulnerabilities of pupils, including pupils with special educational needs or disabilities. It will respond to new technologies and patterns of risk without relying on alarming or victim-blaming messages. Pupils will be shown how to report concerns and will understand that filtering and monitoring support safety but cannot remove every risk.

Where pupils use generative artificial intelligence, they will be taught to follow the Trust's approved arrangements, protect personal and confidential information, recognise that outputs may be inaccurate or biased and apply appropriate critical judgement. Detailed requirements for authorised AI use are contained in the Generative Artificial Intelligence Policy.

6. Filtering and monitoring

PVAT will maintain filtering and monitoring arrangements appropriate to the age and needs of pupils, the curriculum, each school's context and the devices and services in use. Filtering is intended to restrict access to illegal, inappropriate and harmful content. Monitoring assists the Trust to identify potentially concerning activity. Neither replaces effective supervision, education or professional judgement.

Responsibilities for strategic oversight, safeguarding input and technical management will be clearly assigned. The Headteacher, Designated Safeguarding Lead and relevant technical lead will work together so that settings are appropriate, alerts are considered by an authorised person and concerns are passed into the correct school process. Access to monitoring information will be limited to roles that require it.

Provision will be reviewed at least annually and following a significant change, incident or identified weakness. The review will consider coverage, configuration, testing, alert handling, educational impact and attempts to circumvent controls. Changes and exceptions will be authorised and recorded. Staff and pupils must not disable, bypass or attempt to bypass approved controls. Requests to unblock legitimate educational material must use the agreed review route.

7. Safe and appropriate use of technology

Users must follow the Cyber Security and ICT Acceptable Use Policy and any age-appropriate acceptable use agreement. Trust accounts and systems must be used for their intended educational or business purpose. Users must not access, create, store or distribute material that is illegal, harmful, discriminatory, abusive or inconsistent with school expectations, and must not interfere with systems, security controls or another person's work or account.

Personally owned devices may only be used for Trust purposes in accordance with approved arrangements. Each school must maintain clear arrangements for pupils' mobile phones, smart watches and other personal devices, consistent with current statutory guidance and the school's behaviour policy. These arrangements will explain whether devices may be brought to school, where they must be stored, the prohibition on their use during the school day except for approved exceptions, and how breaches will be managed. Searching, confiscation and sanctions are governed by the relevant behaviour and school procedures and current statutory guidance. Where an electronic device may contain an indecent image of a child, including an image generated or altered using artificial intelligence, staff must not view, copy, share, forward or delete the image, or ask a pupil to do so. The device must be secured and the concern reported immediately to the Designated Safeguarding Lead, who will determine the next steps under the safeguarding policy and applicable guidance.

New online services, applications and connected devices must be approved through the Trust's established process before use. The review will consider educational purpose, age suitability, privacy, accessibility, security, advertising, account settings and any requirement for a data protection impact assessment.

8. Communication, social media, images and recordings

Trust-related communication with pupils and families must take place through authorised channels and in a professional manner. Staff must not use personal social media accounts, personal messaging services or private contact details to communicate with pupils unless a formally approved arrangement applies. Official social media accounts and websites will be managed by authorised staff with controlled administrator access.

Published content must protect privacy, comply with copyright and consent arrangements and avoid unnecessary personal information. Photographs, video and audio recordings will only be

created, stored, shared or published for a legitimate purpose and in accordance with the relevant privacy notice and Trust arrangements. Staff must not retain pupil images or recordings on personal devices or personal accounts.

Remote or blended learning will use approved platforms. Pupils and families will receive clear expectations concerning participation, communication, recording and use of cameras and microphones. Sessions will not be recorded unless there is a defined purpose, appropriate approval and clear information about use, storage and deletion.

9. Responding to online safety concerns

Online safety concerns should be reported promptly through the school's current reporting route. Where the concern indicates that a child may be at risk of harm, staff must follow the safeguarding policy and report it to the Designated Safeguarding Lead or a deputy without delay. This policy does not replace or modify the procedures in the safeguarding policy for referrals, allegations, low-level concerns, child-on-child abuse, information sharing or external agency involvement.

Where the matter is a technical or acceptable use issue without an identified safeguarding concern, it will be managed through the relevant ICT, behaviour, staff conduct or data breach procedure. The school will consider whether technical action is required, such as securing an account, preserving relevant logs, restricting access or reviewing filtering settings. Staff and pupils must not conduct their own investigation or redistribute harmful material.

Schools will maintain appropriate records of significant online safety incidents, decisions and actions taken, in accordance with safeguarding, behaviour, data protection and records management requirements. Incident themes will be reviewed to identify patterns, vulnerable groups, training needs and any required changes to technical or educational controls.

Detailed reporting routes, contact details and system instructions will be maintained in operational guidance and staff information so they can be updated without amending this policy.

10. Parents, carers and the wider community

PVAT will provide parents and carers with information about the school's online safety expectations, curriculum, reporting routes and the role of filtering and monitoring. Schools may also signpost practical guidance on parental controls, privacy settings, account security and current online risks. Communications will recognise that families have different levels of access, confidence and experience with technology.

Parents and carers should report concerns promptly and should preserve relevant information without forwarding or republishing harmful material. Where a matter is also a safeguarding concern, communication with parents and carers will be governed by the school's safeguarding policy and professional advice.

11. Training, monitoring and review

Staff will receive online safety information at induction and through regular safeguarding and technology updates appropriate to their role. Training will include acceptable use, professional communication, recognising and reporting online concerns, filtering and monitoring responsibilities and relevant emerging technologies. Trustees, senior leaders, Designated Safeguarding Leads and technical staff will receive information appropriate to their oversight or operational responsibilities.

Implementation will be monitored through curriculum review, filtering and monitoring assurance, staff training, incident themes and governance reporting. Each school will complete and record an online safety risk assessment at least annually, and sooner following a significant incident,

material change in technology or identified control weakness. The assessment will consider safeguarding concerns, local and national trends, filtering and monitoring information, curriculum needs and the age, needs, vulnerabilities and circumstances of the pupil population. The policy will be reviewed annually by the Finance, Audit and Risk Committee and sooner where there is a material change in guidance, technology, Trust arrangements or identified control need.

The use of job titles rather than personal names is intentional. Current role-holders and contact details will be maintained through operational records, safeguarding displays, staff information and school communications, ensuring that staffing changes do not make this policy inaccurate.