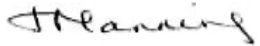




E-Safety Policy

Policy Ref: TMP13v8

This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race, ethnicity or national origin, gender, sexual orientation, marital status, religion or belief, age, disability, socioeconomic status, offending background or any other personal characteristic.

	Name	Title	Signature	Date
Prepared by	Jackie Manning	Principal		July 2026
	Kim Pulman	Director of Pastoral Care		July 2026
Approved by	Martin Heaton	CEO		July 2026

Does this Policy require publishing on the College Website? **Yes**

Does this Policy require approval by Board of Governors? **Yes**

E-Safety Policy

Policy Ref: TMP13v8

Record of Changes

Version	Issue Date	Changes	Initials
v1	July 2019	Initial issue	JM/CF
v2	July 2020	General procedural review, references updated, formatting changes	JM/CF
v3	July 2021	Annual review, references checked and updated	JM/CF
v4	July 2022	Annual review, references checked and updated	JM/CF
v5	July 2023	Annual review, references checked and updated	JM/CF
v6	July 2024	Annual review, references checked and updated	JM/CF
v7	July 2025	Annual review, references checked and updated	JM/CF
v8	July 2026	Updated to align with KCSIE 2026; strengthened online safety, filtering and monitoring, SEND, generative AI, misinformation/disinformation, safeguarding reporting and data protection.	KP/JM

Board of Governors Approval History

Version	Approved by	Signature	Date
v4	Dominic Kohl, Chairman of the Board of Governors		July 2022
v5	Joanne Dockerty Board of Governors		Oct 2023
v7	Claire Bolt, Board of Governors		Feb 2026

Date of Next Policy Review: July 2027

Definition

Throughout this policy document TMP Studios CIC is referred to as 'TMP College'. E-safety and online safety refer to the safe, responsible and appropriate use of digital technology, online services, communications, devices, platforms and emerging technologies, including generative artificial intelligence (AI).

Policy Statement

TMP College recognises that technology is an essential part of education, communication and preparation for adulthood. The College will promote the safe, responsible and positive use of technology while taking proportionate steps to protect learners from online harm.

Online safety is an integral part of safeguarding and is therefore everyone's responsibility. This policy applies to learners, staff, governors, volunteers, contractors and visitors where they use College systems, devices, networks or online services, or where online activity creates a safeguarding concern affecting a learner.

This policy should be read alongside the TMP College Safeguarding and Child Protection Policy, Acceptable Use arrangements, Data Protection arrangements, Photography, Filming and CCTV Policy, Behaviour Policy, Prevent arrangements and relevant staff codes of conduct.

Statutory and Guidance Context

TMP College will have regard to Keeping Children Safe in Education (KCSIE) 2026, Working Together to Safeguard Children 2026, the Prevent Duty Guidance, the Data Protection Act 2018 and UK GDPR as amended by the Data (Use and Access) Act 2025, the Online Safety Act 2023, and Department for Education digital and technology standards, including the filtering and monitoring core standard.

KCSIE 2026 requires all staff to read Part One in full and to follow the College's safeguarding policies and procedures. Staff must act immediately on safeguarding concerns and report them to the Designated Safeguarding Lead (DSL) or Deputy DSL without delay.

Understanding Online Safety

TMP College recognises that online safeguarding risks can occur both on and off College premises and can move rapidly between online and offline environments. Online safety will be considered through the following four broad areas of risk:

Content – being exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm or suicide content, misinformation, disinformation, conspiracy theories, extremist material and AI-generated harmful content.

Contact – being subjected to harmful online interaction with other users, including peer pressure, commercial advertising, grooming, exploitation, coercion, radicalisation and contact from adults posing as children or young people.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, including bullying, abusive or discriminatory behaviour, sharing intimate images, sextortion, harassment, impersonation and misuse of AI or manipulated media.

Commerce – risks including online gambling, inappropriate advertising, phishing, scams, financial exploitation and other harmful commercial activity.

The College recognises that learners with SEND, communication needs, disabilities or other additional needs may experience additional online safeguarding barriers. Online safety education, support and protective arrangements will therefore be adapted to learners' age, developmental level, communication needs, understanding and individual risk profile.

Roles and Responsibilities

The Board of Governors will provide strategic oversight and assurance that appropriate online safety, filtering and monitoring arrangements are in place.

The Principal and Senior Leadership Team will ensure this policy is implemented, staff receive appropriate training and identified risks are acted upon.

The DSL will take lead responsibility for online safeguarding, including understanding the College's filtering and monitoring arrangements and responding to safeguarding concerns arising from online activity.

The College's IT support/provider will maintain appropriate technical controls, provide relevant reports and alerts, and work with safeguarding and senior leaders to address identified risks.

All staff must understand their online safety responsibilities, follow College procedures and report concerns without delay.

Learners are expected to use College technology responsibly and follow the College's acceptable-use expectations.

Teaching and Learning

Online safety will be embedded within the curriculum and tutorial programme rather than treated as a one-off activity. Learners will be supported to develop digital resilience, critical thinking and the skills needed to recognise and respond to online risk.

Learners will be taught what acceptable and unacceptable online behaviour looks like and how to seek help.

Teaching will include privacy, personal information, healthy online relationships, consent, cyberbullying, exploitation, scams, sexual harassment, intimate image abuse, sextortion, radicalisation and harmful online content where age and developmentally appropriate.

Learners will be supported to question the reliability of online information and recognise misinformation, disinformation, conspiracy theories, manipulated media and AI-generated content.

Online safety education will be adapted for SEND and communication needs and reinforced through tutorials, safeguarding education, RSE and Preparation for Adulthood where appropriate.

Staff will model safe, responsible and professional use of technology.

Filtering and Monitoring

TMP College will provide appropriate filtering and monitoring systems to help safeguard learners from illegal, inappropriate and potentially harmful online content and activity. Filtering is preventative and aims to block access to harmful material; monitoring supports the identification of concerning activity and safeguarding risk.

Roles and responsibilities for filtering and monitoring will be clearly identified.

Filtering and monitoring arrangements will be reviewed at least annually by senior leadership, the DSL and IT support/provider, with appropriate Governor involvement.

The review will take account of the learner cohort and risk profile, including age, SEND, communication needs, digital resilience, safeguarding incidents, curriculum requirements, BYOD arrangements and the use of generative AI.

The College will consider whether systems can appropriately address real-time, dynamic, personalised and AI-generated content.

Filtering will not be so restrictive that it unreasonably interferes with teaching, learning or safeguarding access to appropriate information.

Changes to systems, new technologies, significant incidents or emerging risks will trigger additional review where necessary.

Monitoring alerts and reports will only be accessible to authorised personnel and will be handled in accordance with safeguarding and data-protection requirements.

Staff must report concerns about unsuitable sites, inappropriate access, gaps in filtering or monitoring, or concerning online activity promptly.

Generative Artificial Intelligence (AI) and Emerging Technology

The College recognises that generative AI and other emerging technologies can support education but may also create safeguarding, privacy, accuracy, copyright and manipulation risks. New or significantly changed technologies will be assessed before use where appropriate.

Only approved AI tools and services should be used for College purposes where required by College arrangements.

Personal, special-category or safeguarding information must not be entered into unapproved AI systems.

Learners will be taught that AI-generated information may be inaccurate, biased, fabricated or manipulated and should be critically evaluated.

The College will consider DfE generative AI product safety standards when assessing learner-facing AI products.

AI must not be used to create, alter or share abusive, sexualised, discriminatory, deceptive or otherwise harmful content involving learners or staff.

Suspected deepfakes, AI-generated sexual imagery, impersonation or other harmful synthetic media will be treated as safeguarding concerns and responded to accordingly.

Managing Information Systems and Cyber Security

The security of College information systems will be reviewed regularly and appropriate updates and security controls maintained.

Users must use approved accounts and follow password, authentication and device-security requirements.

Suspected phishing, malware, compromised accounts, data breaches or cyber incidents must be reported promptly through College procedures.

Access permissions will be proportionate to role and reviewed where appropriate.

College systems and devices may be monitored lawfully and proportionately for cyber security, safeguarding and acceptable-use purposes.

Email, Messaging, Social Media and Online Communication

College-approved communication systems and accounts must be used for College business with learners unless an authorised alternative is in place.

Staff must maintain professional boundaries and must not use personal social-media accounts or inappropriate private messaging to communicate with learners.

Learners will be supported to protect personal information, location data, passwords and images and to understand the risks of sharing information online.

Offensive, threatening, sexualised, exploitative or otherwise concerning communications must be reported promptly.

Online bullying, harassment, discrimination, coercion and abuse will be managed in accordance with safeguarding and behaviour procedures.

Unauthorised arrangements to meet unknown online contacts must be treated as a potential safeguarding concern.

Published Content, Images and Media

Published content, photographs, video and other media must comply with the TMP College Photography, Filming and CCTV Policy, data-protection requirements and safeguarding expectations. Personal information must not be published or shared in a way that creates unnecessary risk. Permission and the appropriate lawful basis must be established before external publication where required.

Personal Data and Privacy

Personal data will be processed lawfully, fairly and securely in accordance with the Data Protection Act 2018, UK GDPR as amended by the Data (Use and Access) Act 2025, and College data-protection arrangements. This includes data arising from remote learning, CCTV, body-worn camera imagery where used, filtering and monitoring systems, cyber-security monitoring and approved digital or AI services.

Where filtering or monitoring systems process personal data, access to alerts and reports will be restricted to authorised staff, appropriate retention arrangements will apply, and a Data Protection Impact Assessment will be considered before introducing a new system or making significant changes to an existing one.

Internet Access and Acceptable Use

Access to College technology and internet services is subject to the College's acceptable-use expectations. Learners will be supported to understand these expectations in an accessible way. Breaches will be responded to proportionately, taking account of safeguarding, SEND, capacity, context and the learner's understanding. A safeguarding response will take priority where behaviour indicates that a learner may be at risk of harm or exploitation.

Responding to Online Safety Concerns

Online safety concerns are safeguarding concerns where they indicate that a learner may be at risk of abuse, neglect, exploitation or other harm.

Staff must act without delay and report safeguarding concerns to the DSL or Deputy DSL in accordance with the College Safeguarding and Child Protection Policy.

Urgent concerns must be verbally escalated and must not be left solely as an electronic record.

If a learner or another person is in immediate danger, staff should call 999 and inform the safeguarding team as soon as possible.

Staff must preserve relevant information or evidence where appropriate but must not investigate safeguarding concerns themselves, ask leading questions or unnecessarily view, copy or share harmful or sexual imagery.

Concerns involving staff conduct must be managed under the College procedure for safeguarding concerns or allegations about staff and low-level concerns, as applicable.

Online incidents that do not meet a safeguarding threshold may be addressed through behaviour, disciplinary, IT or pastoral procedures as appropriate.

Prevent and Online Radicalisation

TMP College recognises that the internet, social media, gaming, messaging platforms and other online spaces may be used to expose individuals to extremist narratives or facilitate radicalisation.

Staff will remain alert to changes in online behaviour, concerning content, contacts or language and will report Prevent-related concerns through safeguarding procedures. The College's approach will be proportionate, evidence-informed and consistent with the Prevent Duty and safeguarding principles.

Staff Training and Awareness

All staff will receive safeguarding and online safety information at induction and regular updates thereafter. Training will include the College's filtering and monitoring arrangements, how to recognise online safeguarding concerns, reporting routes, professional boundaries, data protection and relevant emerging risks. Staff with specific responsibilities for filtering, monitoring or technical systems will receive training appropriate to their role.

Communication with Learners, Parents and Carers

Learners will receive accessible online safety education, reminders, tutorials and support appropriate to their needs.

Parents and carers will be provided with information and guidance about relevant online safety risks and College expectations where appropriate.

The College will work with learners, families and external agencies where online risks require coordinated safeguarding support.

Monitoring, Review and Governance

This policy and the effectiveness of the College's online safety arrangements will be reviewed at least annually and sooner where there is a significant safeguarding incident, change in technology, change in working practice, change to statutory guidance or an identified weakness in filtering or monitoring. Relevant findings and actions will be reported through the College's safeguarding and governance arrangements.

Key References

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Prevent Duty Guidance for England and Wales
- DfE Meeting digital and technology standards in schools and colleges – Filtering and monitoring core standard
- DfE Generative AI: product safety standards
- Online Safety Act 2023
- Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025