

Online Safety Policy 2026/2027
Including staff and learner acceptable use of ICT policies



Version/Revision	Date	Change	Author
Revision 8	March 2023	Policy reviewed.	VLM
Revision 9	July 2024	Revision/QA	VLM
Revision 10	September 2026	Updated to KCSIE 2026 and DfE Filtering & Monitoring core standard 2026	VLM

 michaeljohntraining
  mjts_manchester
  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#) [#Diveristymatters](#)



Contents

1. Introduction and Purpose	3
2. Roles and Responsibilities.....	4
3. Management of Online Learning and Delivery	7
4. Management of Allegations of Abuse Made Against Educators, Staff and Volunteers	9
5. IT Support and Technology Management (Including Filtering and Monitoring)	10
6. Commitment to The Prevent Duty.....	12
7. Appendix 1: Acceptable Use Policy (Learners, Parents, and Salons)	13
8. Appendix 2 Acceptable Use Policy (Staff)	14

 michaeljohntraining
  mjts_manchester
  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism

#Diversitymatters



1. Introduction and Purpose

The use of technology has become an established and integral part of learning with online resources, online delivery, and remote working. Learners and educators have access to technology and resources that significantly and positively impact learning. For example, OneFile e-portfolio, Pivot-Point, Pellcomp, and MJTS resources.

MJTS learners need to develop good skills in using technology to maximise its use as a learning tool and prepare themselves for future employment and careers. Learner and staff interviews/inductions including digital literacy screening. MJTS recognise that technology is used as a supportive tool in good teaching & learning however, it is also recognised that online safety is an important aspect of keeping learners safe from harm and to promote a culture of safeguarding. Child sexual exploitation; radicalisation; sexual predation, where technology often provides the platform that facilitates harm. Effective policies and procedures raising awareness and activity putting e-safety into practice are required across MJTS to ensure an effective approach to e-safety and protect MJTS and their users in their use of technology during working hours.

All MJTS staff are Enhanced DBS checked before independently working with learners. In line with Keeping Children Safe in Education (KCSIE), all staff receive appropriate safeguarding and child protection training, including online safety and an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, at induction. Training is regularly updated and safeguarding and child protection updates, including online safety, are provided as required and at least annually.

All staff, including those who do not work directly with children, must read Part One in full and follow MJTS safeguarding policies and procedures.

Concerns regarding online and safe use of technology is considerable, but can be categorised into four areas of risk:

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

Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example child-on-child abuse, 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.



michaeljohntraining



mjts_manchester



@Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)



Conduct: online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, including those generated using AI, and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If pupils, students or staff are at risk from phishing, concerns may also be reported to the Anti-Phishing Working Group.

Online safety is a running and interrelated theme across MJTS safeguarding arrangements, curriculum, staff training, the responsibilities of the Designated Safeguarding Lead and learner engagement. Where generative AI is used, MJTS will consider safeguarding, data protection, intellectual property and product safety risks, including whether filtering and monitoring arrangements are capable of addressing dynamic and AI-generated content.

The combined policies of *Health & Safety*, *Safeguarding and Equality* act as an umbrella to the priorities of technology and e-safety as set out in this and relevant policies. The collection of data and subsequent analysis shall be reported through strategic development, and management reporting to further inform annual priorities via self-assessment, strategic vision/management, and Company Targets.

When learners use the Training School network or MJTS-managed internet-connected devices, appropriate filtering and monitoring systems are used to reduce exposure to illegal, inappropriate and potentially harmful content and activity. Filtering is preventative and monitoring is reactive. Alerts, reports or concerns are escalated promptly to the responsible senior leader and Designated Safeguarding Team in line with the level of risk. Filtering and monitoring do not replace staff supervision or professional curiosity.

Learners may also access the internet through personal mobile data or other connections that are outside MJTS network filtering. Staff must remain vigilant, supervise technology use appropriately and report safeguarding concerns or misuse without delay. Learners are taught through the personal development curriculum, induction, announcements and wider learning how to use technology safely, recognise grooming, exploitation, radicalisation, harmful content and other online risks, and how to report concerns.

2. Roles and Responsibilities

Directors:

The Directors are responsible to the governors for approval of this Online Safety Policy and for ensuring that online safety, filtering and monitoring arrangements are effective and reviewed. In line with KCSIE, the effectiveness of filtering and monitoring will be reviewed at least once every academic year by the senior leadership member responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT support. The review will include checks that filtering is working

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism

#Diversitymatters

appropriately on all relevant internet-connected devices and in all relevant locations, with results and actions recorded. Directors ensure staff understand the systems in place, their responsibilities and how to escalate concerns.

Designated Safeguarding Officers:

Designated Safeguarding Officers are trained in online safety and are responsive to concerns or incidents arising from technology use. The Designated Safeguarding Lead has lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. Staff must report concerns promptly to a named responsible person or DSO/DSL. Staff training includes the expectations, applicable roles and responsibilities for filtering and monitoring, and is updated regularly with safeguarding updates provided at least annually.

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

Responsible persons:

Lesley McCormack: Managing Director/ Designated Safeguarding Manager & Prevent Lead/ Equality Officer

Gabriella McCormack: Education Director/ Designated Safeguarding Officer

Abby Brooker: Deputy Designated Safeguarding Lead

Rachel Smith: Designated Safeguarding Officer/ Employer Engagement.

Responsibilities of the named person and the Designated Safeguarding Team:

- Regular Safeguarding meetings and case reviews.
- Appropriate action of reported e-safety incident (internal)
- Filtering and monitoring provision is reviewed at least once every academic year by the responsible senior leadership member, supported by the Designated Safeguarding Lead and IT support. The review and any actions are recorded and include checks across relevant devices, locations and user groups, consideration of learner risk profiles and emerging technology, including generative AI.

Monitoring arrangements include routine review of reports and prompt escalation of high-risk safeguarding, malicious or technical incidents. Outcomes and actions taken are recorded, and concerns are handled in line with safeguarding procedures.

- Reporting online/safeguarding to Governance meetings and Self-Assessment Report.
- Plan and schedule staff training and update PDP to ensure currency e-safety knowledge and compliance.

Teaching & Learning Managers

Are responsible for curriculum design and delivery. The role of teaching and learning management is to plan E-safety sessions, enrichments and activities as informed by clear intent, implementation and impact of the personal development and wider curriculums. Responsibility is to ensure learners are aware and informed of the organisation's policies and procedures while disseminating awareness and resources to keep learners vigilant to the dangers of using technology while staying safe when being active online and using social media.

Vigilance to e-safety also considers the visual display and information for learners regarding e-safety. Announcements will be appropriately shared with learners during registration. Throughout delivery, messages are underpinned and supported by screen displays in the corridors. Learner surveys and feedback from sessions planned into the curriculum, also check awareness and compliance toward e-safety through structured teaching and learning activities.

Overview of Teaching & Learning Management responsibilities:

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

- Ensure e-safety is embedded into personal development design and delivery through sessions and enrichments.
- Ensure staff are disseminating up-to-date awareness of policy and procedure of e-safety to all learners.
- Ensure learners and staff are aware and responsible for e-safety compliance when using technology devices (mobile phones & cameras)

Learners:

Considered as anyone enrolled on an MJTS program of learning. The learner will confirm their obligation and understanding of the technology and e-safety policies at Induction. Agreement underpins their full acknowledgement and attendance of planned session delivery to continuously update and support further learning and development of knowledge in this area.

Responsibilities of Learners:

- Comply with the policies and procedures of technology and e-safety throughout their learning and ensure that learners follow the Training School's Acceptable Use Policy (Appendix 1)
- Keep usernames and passwords safe for all MJTS resources and applications associated with their learning (MJTS website as a learner, Pivot Point Labs resources, logging onto Pc's and laptops, using the WIFI... this list is not exhaustive)
- Undertake initial assessment and online learning as directed.
- Ensure respect and consideration are shown to staff and peers when using technology staying e-safe as individuals supporting a whole organisational approach for e-safety.
- Use technology effectively to research safely and without plagiarism or infringement of copyright.
- Be confident in policies, remain vigilant and feel confident and safe in reporting indecent activity, incidents, abuse, or breaches experienced or associated with technology or e-safety (at MJTS or in personal use)
- Be confident in how the policies for technology, e-safety are in place to protect learners and learning (at MJTS or in personal use) and understand the consequence of misuse.

Responsibilities of Employer/Salon

- Support MJTS OTJ activities as applicable by providing safe technology and e-safety where appropriate.
- Contact MJTS for support and advise/reporting.

3. Management of Online Learning and Delivery

 michaeljohntraining
  mjts_manchester
  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

Use of technology for online/ virtual teaching.

Online Learning is monitored and assured by the Directors as Designated Persons, Health & Safety and Equality Officers. All online content delivered by MJTS is done using a company, laptop/computer, Microsoft 365 email and VPN access (when required, set up by our IT Service Provider). Where a non-organisational device is used. Consent must be agreed by Senior Management and the device will be required to use the company Microsoft 365 email along with VPN access to the company network.

Contact by phone must be made using the recognised Michaeljohn contact number, sanctioned and set up as agreed by Directors/Managers. In the unlikely event it is not possible for the Phone System to be used, MJTS staff MUST use the MJTS text messaging service. If a learner requires a phone call, personal numbers are set to private. This MUST be authorised by your Line Manager. Communications through social media will also take place via the MJTS accounts.

However, OneFile will be the main source of communication between Educators and learners.

WhatsApp to learners via a staff members personal device or personal social media accounts is a breach of policy including safeguarding policy and will lead to disciplinary action/dismissal.

Virtual teaching (Live demonstration) online using social media (Instagram, YouTube) must be as agreed by Teaching & Learning management via MJTS registered accounts and recorded.

Staff MUST display the same standards of dress and conduct that they would display at MJTS or in salon. They should act as role models for learners. Staff should follow the MJTS Code of Conduct at all times.

- Sessions delivered must be recorded or observed.
- Staff and learners must wear suitable clothing, this includes anyone else who may be in scope of the camera
- Language must be professional and appropriate (as with anyone else who may come into the scope of the camera).
- Staff should operate from communal areas (office, lounge, dining room, conservatory etc.) never from a bedroom.
- What is in the background of their screen (photos, artwork, personal artefacts, mirrors, books) ideally you should operate with an appropriate false or blurred background.
- Ensure connectivity is robust.
- Keep sessions to a reasonable length of time to ensure learner engagement and concentration. (Recording duration, date, and time of attendance)

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism #Diversitymatters

- Ensure that resources and reference material are either of the agreed online learning resource or have been agreed for use with a Line Manager, used by policies and procedures of the organisation.
- Monitor and assess the level of anxiety or distress a learner may display, reporting to Safeguarding where it may be apparent the learner is showing mental health issues.
- Recording of the session must be included in the 20% monitoring of OTJ, inform of impact and include any additional support required.

MJTS STAFF (teaching & learning, Recruitment & Quality Department)

Responsible for the Teaching & Learning Management and reporting to Senior Leadership, MJTS staff are to ensure they remain vigilant to the policies and procedure. MJTS staff are responsible for the monitoring, support, information, advice, and guidance and reporting issues for learners and users following this policy. All staff are encouraged to share and inform best practices to improve Teaching & Learning Management, escalating to named responsible persons where appropriate and without delay.

4. Management of Allegations of Abuse Made Against Educators, Staff and Volunteers

Cross reference to MJTS Child Protection, Safeguarding and PREVENT Policy.

Any allegation of abuse or inappropriacy shall be investigated thoroughly and the appropriate action is taken. To reduce the likelihood of false allegations, the following staff behaviours are expected of all staff representing MJTS (including volunteers).

Be aware that contact or communication with any former employee regarding company business via MJTS technology, either casual or unconstrained, may be considered unfavourable to the interests of the company or incumbent members of staff. This may lead to preventative or legally restraining action being made upon the employee or former employee and may lead to disciplinary action.

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)



5. IT Support and Technology Management (Including Filtering and Monitoring)

Ark Technology Group installs, updates, monitors, and manages our IT infrastructure remotely (with a quarterly site visit) under a dedicated IT Service Contract. Ark also monitors and supplies the antivirus, firewall, web filtering and any form of access to the IT systems. BT supplies dedicated broadband with a guaranteed speed of 100Mbps. MJTS VoIP phones are supplied and supported by Fidelity Group which monitors and updates the systems. MJTS Wi-Fi is accessed with a secure SSID and password. VPN access is granted on a user-by-user basis with the written consent of a director.

MJTS will ensure that filtering and monitoring arrangements meet the DfE Filtering and Monitoring core standard and KCSIE, taking account of the age and risk profile of learners, SEND and EAL needs where relevant, how and where devices are used, and the safeguarding implications of generative AI and other emerging technologies.

Responsibilities of IT support and technology management:

- The responsible senior leadership member, Designated Safeguarding Lead and IT support will work together to manage filtering and monitoring. Roles, escalation routes and responsibilities will be clearly assigned and understood.
- Filtering and monitoring provision will be reviewed at least once every academic year. The review will identify current provision, gaps, learner and staff needs, additional checks required, and any actions. Results will be recorded and made available for appropriate scrutiny.
- Filtering checks will confirm that protection is operating appropriately on all relevant internet-connected devices and in all relevant locations. MJTS will understand the system's coverage and limitations and mitigate risks that filtering cannot address.
- Filtering must block harmful and inappropriate content without unreasonably restricting teaching, learning or administration. Appropriate access profiles will be used for different user groups rather than relying on one blanket profile for all users.
- Filtering provision will include appropriate controls for illegal content and relevant blocklists, including child sexual abuse material and terrorist content, and these protections must not be capable of being disabled, overridden or altered by ordinary users.
- MJTS will consider safe-search controls, personal or bring-your-own devices used for learning, technologies that may reduce the effectiveness of filtering, and whether solutions can address real-time, dynamic, personalised and AI-generated content.
- Monitoring will be proportionate to MJTS safeguarding needs and may include staff supervision, network logs and technical monitoring. Monitoring does not itself prevent unsafe activity, so effective supervision and staff awareness remain essential.

 michaeljohntraining  mjets_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism

#Diversitymatters

- As a minimum, monitoring arrangements will provide routine reports highlighting incidents and immediate escalation where an incident is classed as high risk. There will be a documented process for recording incidents, action taken and outcomes.
- Users will be made aware that filtering and monitoring processes are in place. Where technical monitoring is used, appropriate notices will be provided and relevant privacy information maintained.
- Where technical monitoring involves the processing of personal data, MJTS will consider data protection requirements, including an appropriate data protection impact assessment where required, and will review relevant third-party provider privacy information.

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)



6. Commitment to The Prevent Duty

MJTS recognise that young people are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harm and abuse, the curriculum embeds activity to raise awareness and understanding of the risks of radicalisation/extremism and its close association with technology. To ensure learners access and use technology responsibly, safely and appropriately, MJTS combines its Prevent Duty responsibilities with the requirements of Keeping Children Safe in Education and the DfE Filtering and Monitoring core standard. The appropriateness of filtering and monitoring is informed in part by the Prevent Duty risk assessment. Full commitment to how MJTS meets its Prevent Duty obligations is outlined in the PREVENT Risk Assessment.

Much of this policy's purpose and scope, addresses and supports the principles of Prevent, below are specific commitments aligned to the policy.

- Through monitoring of behaviours and the use of technology, all staff are required to be vigilant and responsive to the ideological challenge of terrorism/ radicalisation and extremism. Under this policy and safeguarding, where you have the slightest concern, report it to a Designated Safeguarding Officer.
- Curriculum delivery of safety using technology is delivered through Intent, Implementation and impact ensuring that the message of 'staying safe online' extends to 'being vigilant' to what a learner may see, or how peers may be behaving. Technology must always be monitored to prevent young people from being drawn into terrorism, ensuring that learners are given appropriate advice and support.
- Good and effective communication and cooperation with agencies and inter agencies, sharing resources and advice, guidance and messages from the Counter Terrorism Police, MJTS wish to contribute and minimise the risks of extremism and radicalisation in our programmes. Monitoring of Technology is one such way to help defeat extremism and radicalisation. All staff have a responsibility to report any concerns they may have to a Designated Safeguarding Officer, who will consult the Greater Manchester Police prevention team if the principles of the Prevent Duty have been breached.

7. Appendix 1: Acceptable Use Policy (Learners, Parents, and Salons)

We have named persons responsible for ensuring the technology in the Training School is safe, monitored, and robust in preventing harmful materials from affecting your learning and your time with us:

Main Responsible Person

Lesley McCormack: Managing Director/ Designated Safeguarding Lead/Equality Officer

Supported by:

Gabby McCormack : Education Director

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

Abby Brooker : Recruitment Manager & Strategic Lead

Rachel Smith : Employer Engagement Officer

A clear pledge to all learners; Michaeljohn Training School supports and encourages the use of technology in your learning. That may include using our resources and IT or your devices.

As an MJTS learner: you are welcome to access IT resources made available to you or supplied as part of your learning (on-site or for personal use). You must always be respectful of the property you are using and adhere to the Training School rules and policy. Through policy, procedure and learning, learners will be made aware of their responsibilities and the consequence of any misuse of technology at induction and sessions. MJTS, where necessary, will remove ICT that has breached the policy.

Prevention of IT misuse

1. Our IT service provider supports monitoring of the network for unacceptable use. MJTS uses filtering to prevent access to illegal, inappropriate and potentially harmful content and uses monitoring to identify activity that may require safeguarding, technical or disciplinary action. No filtering system is 100% effective; staff supervision, learner education and prompt reporting remain essential.
2. Any suspicious on-site activity detected is reported to the Directors/Managers immediately.
3. Should you experience anything that makes you feel uncomfortable or offended when accessing our technology please report it immediately to the responsible persons.

Learners should understand that activity on MJTS networks and managed devices may be filtered and monitored for safeguarding and security purposes. Personal mobile data may sit outside MJTS network filtering; the same expectations for safe and acceptable use still apply.

Examples of breaches or harmful offensive content are:

Harassment

Bullying

Incitement of extremist/hateful views

Sexually inappropriate language or images

Attempts to take your details.

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

All offensive material will be isolated for the report to our IT provider who will preserve the material to potentially report to external agencies. Once controlled the material will be removed and dealt with by the Designated Safeguarding Team.

8. Appendix 2 Acceptable Use Policy (Staff)

The purpose of this policy outlines Michaeljohn Training School's commitment to ensure staff are clear and informed of the protocols to abide by when using technology as an MJTS employee. This policy will be issued and agreed upon by:

- staff induction
- updated safeguarding and online safety training for all employees, including the expectations, applicable roles and responsibilities in relation to filtering and monitoring, with updates provided as required and at least annually.
- Further training made available throughout the year with online modules.

Training is recorded to individual staff CPD/PDP records for review and further planning (ST5).

The policy is aligned with the associated Learner Acceptable Use of Information Technology Policy outlining the organisation and staff's commitment to keeping our learners safe and aware when using technology. Staff are further informed of the protocols and code of conduct in their use of ICT in the MJTS Online Safety Policy (*which is part of this policy*). ICT resources and systems are supported offsite by our IT service provider, responsible for the security of the local network and server (Ark Technology). Security of anti-virus and firewalls are continuously and professionally monitored, managed and responsive to threats. This is assured by commitment to Cyber Essentials Accreditation.

Unacceptable behaviour

The following examples are deemed unacceptable uses of company technology or access via a personal device at work. Such actions may result in disciplinary action or dismissal:

1. Accessing illegal, harmful or inappropriate materials such as visiting internet sites that contain illegal, obscene, hateful, pornographic, or extremist material
2. Using the technology to perpetrate any form of fraud, break the law or breach of copyright with software, media piracy, banned or illegal sites (such as extremist or dark web sites)
3. Using technology to send offensive or harassing material to other users.
4. Downloading commercial software or any copyrighted materials belonging to third parties unless this download is covered or permitted under a commercial agreement or other such licences.
5. Attempt to introduce nonregulated or malicious software to desktops or the server (admin rights protected)

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

6. Hacking into unauthorised areas or deliberately bypassing any firewalls, spyware or antivirus associated with MJTS technology designed to keep IT systems safe.
7. Publishing defamatory and/or knowingly false material about MJTS, your colleagues and/or our partners on social networking sites or public spaces such as blogs, Vlogs, chat rooms, apps with user-generated comments, wikis, and any online publishing format (this may be considered during both work hours and in your personal life).
8. Any form of social contact and/or relations with learners via social networking sites, blogs (online journals), or wikis, must in the first instance, be sanctioned by a director as appropriate for learning or organisation activities. No sanctioned activity is prohibited under the terms of the policy. Action that is not declared before the activity is considered a breach of policy and may lead to disciplinary action.
9. None-declared or unauthorised communication with a young person through any form of technology, where the employee association is because of the young person being a current/former learner of MJTS, is also prohibited under the terms of the policy unless sanctioned by a director in the interest of learning or organisational activities.
10. Undertaking activities through technology, that deliberately/indirectly wastes time and resources is a breach of policy.
11. Use of removable media such as pen drives/ USB memory to take/store company documentation and resources for purposes outside company objectives is a breach of policy (all staff have access to MJTS Office 365, this allows the legitimate transfer of documents without the need of any of the above devices). Breaching this may lead to disciplinary action/dismissal.
12. Sharing or giving out passwords with other staff or users compromising security, accountability and monitoring of technology is in breach of this policy (Any disclosure or use must have a director's sanction).

Company-owned information held on third-party websites.

Any file, document or information created, collected, processed, or uploaded relating to MJTS operations or intellectual property, produced in the course of your employment, remains the property of MJTS. As such, this should therefore be made accessible to colleagues via identified access rights on the MJTS server (documents on MJTS PC desktops will not be as readily accessible without the know password or login). Such property includes any information stored on networking partners and agencies sites (such as the Apprenticeship Site). Unless sanctioned by a director, intellectual property should not be shared with any third-party websites such as webmail service providers or social networking sites, such as Facebook, Twitter, and LinkedIn. All staff have a clear and transparent Microsoft 365 account which is transferable but can be monitored by the organisation.

The policy requires you to abide by and understand that the **Data Protection Policy** requires that any personal data to which you have access, will be kept private and confidential, except when it is

 michaeljohntraining
  mjts_manchester
  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism

#Diversitymatters

deemed necessary that if required by law or by MJTS policy, you disclose such information to appropriate persons or authority.

Monitoring

MJTS accepts that technology is a valuable educational and business tool. To protect learners, staff, systems and the organisation, use of MJTS networks, managed devices, Microsoft 365 and other business systems may be filtered and monitored in accordance with safeguarding, security and data protection requirements. Monitoring may include review of internet and network activity, alerts and reports generated by technical systems, and investigation of suspected misuse. High-risk safeguarding, malicious or technical incidents will be escalated promptly to the appropriate responsible person. Staff must understand that monitoring does not replace their duty to supervise learners, remain professionally curious and report safeguarding concerns to the Designated Safeguarding Lead.

MJTS will maintain a documented process for recording monitoring incidents, actions and outcomes, and will ensure relevant privacy information and data protection assessments are kept under review where technical monitoring processes personal data.

Sanctions

If it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to Instant dismissal. The penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

As an organisation, MJTS takes responsibility for performance towards a government contract very seriously. In acknowledging responsibility and our duty of care in ensuring young people succeed in a safe environment, MJTS complies with legislation, statutory guidance and best practices as required under government-funded Training Provisions. We will always consult and adopt the requirements of government policies and the inspectorate best practice over our organisational recommendations, should we have cause to implement sanctions on an employee's breach or irregularity through misuse of technology concerning *Health & Safety, Safeguarding or Equality*. In the unlikely event of such an instance, the severity may require informing government inter agencies leading to prosecution.

*Staff and learners will be asked to sign the Acceptable use of ICT Declaration.

3. Governance and assurance

The Managing Director, senior leadership team and DSL will monitor implementation of this addendum.

Assurance activity will include:

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

#Communitiesdefeatterrorism

#Diversitymatters

- Annual online safety risk assessment
- Annual filtering and monitoring effectiveness review
- Review of AI tools and digital platforms
- Review of mobile phone arrangements
- Staff training and reading declarations
- Learner feedback and safeguarding voice
- Analysis of online safety incidents and near misses
- Employer and partner feedback
- Cyber-security incident reviews
- Evidence of actions taken and their impact
- Reporting to governors or the appropriate oversight body

MJTS will record actions arising from reviews and assign each action an owner and completion date.

This Online Safety Policy Addendum was approved by Michaeljohn Training School on or after 1 September 2026. It reflects the online safety, artificial intelligence, filtering and monitoring, cyber-security, mobile-device and safeguarding requirements introduced or strengthened by Keeping Children Safe in Education 2026. It will be reviewed at least annually and incorporated into the School's comprehensive Online Safety Policy at the next scheduled policy review.

This addendum gives Michaeljohn Training School a focused September 2026 update without duplicating the existing comprehensive policy. Its main additions are AI-enabled harm, deepfakes, annual documented filtering and monitoring reviews, cyber security as safeguarding, mobile-phone-free expectations, stronger online child-on-child abuse procedures, and expanded staff, learner, employer and partner responsibilities.

On Behalf of Michaeljohn Training



Lesley McCormack: Managing Director

This policy will be reviewed annually or sooner should legislation/changes require.

ORGANISATION AND EMPLOYEE AGREEMENT

All company employees, contractors, temporary staff or volunteers who have been granted the right to use the company's internet access are required to sign this agreement confirming their understanding and acceptance of this policy.

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)

Employee Signature

Employee Name.....

Date of Agreement.....

Volunteer Signature

Volunteer Name.....

Date of Agreement.....

This policy has links to the following policies;

Child Protection, Safeguarding and PREVENT Policy

Equality Policy

PREVENT Duty Risk Assessment

DfE Filtering and Monitoring: core standard (2026)

Keeping Children Safe in Education

 michaeljohntraining  mjts_manchester  @Michaeljohn_mcr

MJTS is an Equal Opportunities Training School. We welcome people from all backgrounds and believe in treating people according to their needs. MJTS is committed to a whole organisational approach to Safeguarding, 'Personal Development' and 'Behaviour and Attitudes'.

Rev 10/September 26

[#Communitiesdefeatterrorism](#)

[#Diversitymatters](#)