MEPA ACADEMY

ACCEPTABLE USE POLICY

Policy owner	Principal / Senior Attendance Champion
Approved by	Senior Leadership Team
Adopted	July 2026
Review date	July 2027, or sooner if guidance changes
Applies to	All pupils aged 11-16, staff and any users who has access to computers and wifi.

Contents

Policy statement 3
1. Purpose 3
2. Scope 3
3. Governance and responsibilities 3
3.1 Headteacher and senior leadership team 3
3.2 SLT Digital Lead 4
3.3 Designated Safeguarding Lead 4
3.4 Data Protection Officer 4
3.5 IT support 4
3.6 All staff 4
3.7 Users 4
4. Acceptable use requirements 5
4.1 Accounts and access 5
4.2 Safe, lawful and respectful conduct 5
4.3 Email, messaging and collaboration 5
4.4 Software, storage and equipment 5
5. Filtering and monitoring 6
5.1 Technology and purpose 6
5.2 Coverage and configuration 6
5.3 Review, checking and response 6
6. Monitoring, privacy and records 6
7. Bring your own device and guest access 7
8. Generative AI and emerging technology 7
9. Education, training and communication 7
10. Reporting and incident response 8
11. Breaches and sanctions 8
12. Approval, review and assurance 8
Standards and guidance considered 9

Policy statement

MEPA Academy provides digital technology to support education, safeguarding, communication and administration. All use must be safe, lawful, respectful, proportionate and consistent with the Academy's educational purpose. This policy defines the Academy's governance and controls and the responsibilities of everyone who accesses its accounts, data, devices, networks or digital services.

Relationship to the student agreement. The Student Acceptable Use Agreement is the age-appropriate user agreement made under this policy. It should be explained and acknowledged at the start of each academic year and whenever materially updated.

1. Purpose

The policy aims to:

- protect children and adults from online harm and support the Academy's safeguarding duties;
- protect personal data, systems and services from accidental or deliberate misuse;
- set clear, fair and age-appropriate expectations for users;
- make filtering and monitoring transparent and effective;
- support teaching, learning, accessibility and digital resilience without unreasonable restriction; and
- provide consistent routes for reporting, investigation, support and proportionate action.

2. Scope

This policy applies to students, staff, governors or trustees, contractors, volunteers, supply staff, visitors and any other authorised user. It covers:

- Academy-owned, leased or managed devices, wherever used;
- Academy accounts, email, Microsoft Teams, cloud services, learning platforms, applications, storage and data;
- wired, wireless, guest and BYOD network access;
- personal devices used on Academy premises, connected to Academy internet access, or used for Academy-related activity; and
- online conduct outside the Academy where there is a safeguarding concern, an impact on the Academy community, or a connection to Academy systems, people or reputation.

This policy should be read with the safeguarding and child protection, behaviour, online safety, staff code of conduct, data protection, privacy, records retention, remote learning, BYOD, disciplinary, business continuity and incident-response policies.

3. Governance and responsibilities

3.1 Headteacher and senior leadership team

- ensure appropriate resources, training, policies and procedures are in place;
- appoint an SLT Digital Lead and establish clear decision-making and escalation routes;
- approve what categories or services are blocked or allowed and record the rationale;
- ensure relevant agreements are communicated and acknowledged; and
- coordinate proportionate responses to serious misuse or cyber incidents.
- approve this policy and receive assurance that it is implemented;

- retain overall strategic responsibility for appropriate filtering and monitoring;
- identify a responsible governor or trustee; and
- receive the outcome of the annual filtering and monitoring review and significant risk or incident reporting.

3.2 SLT Digital Lead

- own this policy and coordinate its annual review;
- lead the digital strategy, cyber-risk assessment and improvement plan;
- work with the DSL, DPO and IT support on filtering, monitoring, procurement and risk;
- ensure approved applications, systems, access controls and technology registers are maintained; and
- report material risks and gaps to senior leaders and governors or trustees.

3.3 Designated Safeguarding Lead

- lead on safeguarding and online safety;
- review relevant monitoring reports and high-risk alerts;
- make sure concerns are recorded, assessed and acted on promptly under safeguarding procedures;
- inform the filtering and monitoring risk profile, training and review; and
- provide safeguarding assurance to leaders and governors or trustees.

3.4 Data Protection Officer

- advise on lawful bases, transparency, data minimisation, retention, access and sharing;
- advise on and review data protection impact assessments where required;
- review supplier privacy information and data-processing arrangements; and
- support personal-data breach assessment and reporting.

3.5 IT support

- configure, maintain and test filtering, monitoring, identity, device and security controls;
- provide understandable reports and urgent alerts to authorised staff;
- keep technical documentation, approved software lists and relevant logs;
- act promptly on faults, incidents, vulnerabilities and approved change requests; and
- work with the DSL and SLT Digital Lead when checks or reports identify concern.

3.6 All staff

- model appropriate use, supervise students and reinforce the student agreement;
- use Academy accounts and approved systems for Academy business;
- protect information and report safeguarding, cyber-security and data-protection concerns promptly; and
- complete required training at least annually and after material changes or identified risks.

3.7 Users

Every user must understand and follow the relevant acceptable use terms, protect credentials and devices, respect others and report concerns. Staff, contractors, visitors and other adults should receive role-appropriate terms in addition to the student agreement.

4. Acceptable use requirements

4.1 Accounts and access

- Use only the account and access privileges issued to you; do not share passwords, passcodes or multi-factor authentication codes.
- Use unique, strong passwords or passphrases that meet the Academy's current technical policy; suspected compromise must be reported immediately.
- Lock or sign out of unattended devices. Lost, stolen or misconfigured devices and accounts must be reported promptly.
- Do not access, attempt to access, change, copy or delete systems or data without authorisation.
- Privileged access must be limited, separately controlled and used only for authorised administrative activity.

4.2 Safe, lawful and respectful conduct

- Use Academy technology primarily for authorised education or Academy business. Limited personal use by staff may be permitted where it is lawful, reasonable, does not interfere with duties and does not create cost or risk.
- Do not create, access, store or share illegal, sexual, hateful, extremist, abusive, discriminatory, defamatory, malicious or otherwise harmful material, except where specifically authorised for a legitimate safeguarding, curriculum or professional purpose with suitable controls.
- Do not bully, harass, threaten, impersonate, groom, shame or deliberately exclude others.
- Protect personal, confidential and safeguarding information; disclose it only through approved channels to people with a legitimate need.
- Respect copyright, licences, attribution, examination rules and intellectual property.
- Do not capture, record, alter or distribute another person's image, audio, video, messages or work without an appropriate lawful basis and permission.

4.3 Email, messaging and collaboration

- Use Academy-approved accounts and channels for Academy communications.
- Do not send spam, chain messages, unauthorised mass communications or commercial promotions.
- Treat unexpected links, attachments, login prompts, payment requests and requests for information as suspicious; verify through a separate trusted channel and report concerns.
- Live sessions must be authorised, appropriately supervised and configured. Recording requires an approved purpose, prior transparency and appropriate permissions.
- Communications must remain professional, proportionate and capable of appropriate oversight.

4.4 Software, storage and equipment

- Install or use only approved software, applications, extensions, devices and storage services.
- Do not alter settings, disable security controls, connect unauthorised removable media or attempt repairs without approval.
- Store Academy information only in approved locations and apply the relevant access, sharing, classification and retention requirements.
- Handle equipment responsibly and report faults, damage, loss or suspected malware promptly.

5. Filtering and monitoring

5.1 Technology and purpose

MEPA Academy uses Lightspeed Filter as its technical filtering solution and as part of its technical monitoring arrangements. It is supported by classroom supervision, staff awareness, reporting routes and other proportionate technical or manual controls. The Academy does not assume that any filtering or monitoring system is completely effective.

Filtering is preventative: it restricts access to illegal, harmful or inappropriate content. Monitoring is reactive: it helps authorised staff identify and respond to safeguarding, harmful-content, misuse and cyber-security concerns. The provision must support, rather than unreasonably obstruct, teaching and learning.

5.2 Coverage and configuration

- Filtering will be age-, role- and context-appropriate, with distinct profiles for students and staff.
- Academy-managed devices will be protected on site and, where technically supported and risk-assessed, off site.
- Guest and personal devices using Academy internet access will use a separate, appropriately filtered network.
- Users must not bypass filtering or monitoring through VPNs, proxies, hotspot connections, unauthorised browsers or extensions, encryption techniques used to evade controls, or other methods.
- Safe-search and browser controls will be applied where appropriate, and users will not be permitted to change protected settings.
- Changes to blocks, allowances and monitoring rules must be authorised and documented.

5.3 Review, checking and response

- The SLT Digital Lead, DSL, IT support and responsible governor or trustee will review filtering and monitoring at least once each academic year.
- A review will also take place after a significant safeguarding risk, new technology or generative-AI deployment, major software or configuration change, or a change such as remote access or BYOD.
- Checks will cover relevant sites, device types, locations, connections and user profiles. A log will record who checked what, when, the result and any action.
- The monitoring plan will provide routine reports at least weekly and immediate escalation for high-risk incidents, subject to the Academy's risk assessment and configuration.
- Staff will know how to report over-blocking, under-blocking, system failure, suspected evasion and safeguarding concerns.

6. Monitoring, privacy and records

Use of Academy accounts, services, networks and managed devices may be logged and monitored, including through Lightspeed Filter. Depending on the system and Academy-approved configuration, records may include user and device identifiers, dates and times, websites or search terms, communications metadata, content or activity that triggers a concern, and actions taken in response.

Monitoring must be necessary and proportionate. The Academy will identify and document an appropriate lawful basis, provide clear privacy information, minimise the information collected,

restrict access, set retention periods, secure records and share information only where lawful and appropriate. A data protection impact assessment will be completed or reviewed where required, including for technical monitoring or significant new technology.

Consent or signature is not relied upon as the sole lawful basis for routine monitoring. Refusal to sign an agreement does not remove the Academy's safeguarding, education, employment or data-protection duties. Requests concerning personal data should be directed to the DPO.

7. Bring your own device and guest access

- BYOD is permitted only where authorised and subject to the Academy's risk assessment and published arrangements.
- Personal and guest devices must use the designated network and must not connect to the wired or protected internal network unless explicitly authorised.
- Users remain responsible for secure configuration, updates, physical security and lawful use of their device.
- The Academy may restrict, quarantine or remove network access where a device presents risk or breaches policy.
- Academy information must not be stored on personal devices unless expressly approved and protected.
- Any examination, accessibility, safeguarding or staff-use exception must be documented and appropriately controlled.

8. Generative AI and emerging technology

- Only Academy-approved generative-AI tools may be used with Academy accounts, systems, data or work, and students require staff authorisation for the task.
- The SLT Digital Lead, DSL, DPO, curriculum leads and IT support will assess safeguarding, data-protection, security, accessibility, age, intellectual-property and teaching risks before approval.
- Personal data, confidential information, safeguarding information, assessment material and another person's work must not be entered into AI systems unless that specific use has been approved.
- Users must verify outputs for accuracy, bias, harmful content, fabricated information and copyright concerns; the human user remains accountable.
- AI assistance must be acknowledged where required and must comply with assessment and examination rules.
- AI must not be used to impersonate, deceive, bully, sexualise or create harmful or misleading synthetic media about any person.
- Filtering and monitoring limitations for dynamic, personalised and AI-generated content will be considered in the annual review and whenever a new AI tool is introduced.

9. Education, training and communication

- Students will receive age-appropriate online-safety and cyber-security education, reinforced through the curriculum and the student agreement.
- Staff and relevant adults will complete training at least annually and more frequently where risk requires. Training will cover phishing, password security, social engineering, physical device security, removable media, multi-factor authentication, incident reporting, personal-data breaches and safeguarding.
- At least one current governor or trustee will receive relevant cyber-security awareness training.

- Parents and carers will be informed about the student agreement, filtering and monitoring, reporting routes and safe home use where Academy devices or services are used remotely.
- Visitors, contractors, volunteers and temporary staff will receive proportionate terms before being given access.

10. Reporting and incident response

Users must report safeguarding concerns, inappropriate access, suspicious communications, compromised credentials, malware, data loss, device loss, control failure and suspected unauthorised activity immediately through the appropriate Academy route.

1. Make the situation safe without forwarding harmful material or conducting an unauthorised investigation.
2. Preserve relevant information and logs where lawful and necessary.
3. Escalate safeguarding matters to the DSL and technical matters to IT support; involve the DPO where personal data may be affected.
4. Assess severity, contain risk, support affected people, record decisions and actions, and notify leaders or external bodies where required.
5. Review the incident for lessons, control changes, training needs and any necessary policy update.

Students will not be disciplined for accidental access that is reported promptly and handled responsibly. Staff must not promise confidentiality where safeguarding or legal duties require information to be shared.

11. Breaches and sanctions

Suspected breaches will be considered fairly, proportionately and in context, including intent, impact, repetition, role, age, needs and safeguarding considerations. The Academy may provide guidance or support, preserve evidence, restrict access, require training, contact parents or carers, apply behaviour, capability, disciplinary or contractual procedures, and refer serious or unlawful matters to safeguarding partners, the police, regulators or other authorities.

Financial liability for loss or damage is not automatic and will be considered under the Academy's published arrangements, contractual terms and applicable law. Access needed for education, accessibility or safeguarding will be managed proportionately.

12. Approval, review and assurance

- The governing body or trustees approve this policy following consultation with the Headteacher, SLT Digital Lead, DSL, DPO and IT support.
- The policy and related user agreements will be reviewed at least annually and after material legal, guidance, technology, safeguarding or operational change.
- The annual review will consider incidents, training completion, user feedback, accessibility, filtering and monitoring checks, supplier assurance, DPIAs, cyber risks and gaps against the DfE standards.
- Material non-compliance or control gaps will be recorded with an owner, target date, interim mitigation and route for escalation.

Standards and guidance considered

- DfE, Meeting digital and technology standards in schools and colleges: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- DfE, Filtering and monitoring: core standard: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- DfE, Cyber security: core standard: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard
- DfE, Data protection in schools: https://www.gov.uk/guidance/data-protection-in-schools
- DfE, Generative AI: product safety standards: https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards