Mulberry Park Educate Together

Online Safety Policy

September 2026

Approval by:	Local Governing Board
Date of approval:	September 2026
Review date:	September 2027

Version	Date	Summary of changes	Author
1.0	September 26	National College template used as a basis, supported by Acorn Health and Safety	Sarah Phillips

Contents

1. Introduction and scope
2. Policy development, monitoring and review
3. Policy and leadership
4. Online Safety Group
5. Policy and acceptable use
6. Reporting and responding
7. School actions and sanctions
8. Use of Artificial Intelligence (AI)
9. Online Safety Education Programme
10. Staff, governors, parents/carers and external stakeholders
11. Technology
12. Filtering and monitoring
13. Technical and cyber security
14. Data protection
15. Technology practice and device management
16. Digital content, images and video
17. Public online communications and social media
18. Outcomes
19. Related policies and appendices

1. Introduction and scope

This Online Safety Policy outlines MPET's commitment to safeguard members of the school community online in accordance with statutory guidance and best practice. Online safety is an integral part of safeguarding and is a shared responsibility across the school community.

This policy applies to all members of the school community, including staff, learners, governors, volunteers, parents and carers, visitors and community users who have access to, or use, school digital systems. It applies to the use of school systems both on and off site and to the use of personal digital technology on the school site where permitted.

Where online safety concerns or incidents occur outside school and are known to MPET, the school will respond in line with this policy and associated safeguarding, behaviour and anti-bullying procedures. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place outside school.

MPET recognises the four broad areas of online safety risk described in Keeping Children Safe in Education: content, contact, conduct and commerce. These areas will inform safeguarding practice, curriculum planning, staff training and review activity.

2. Policy development, monitoring and review

MPET will monitor the impact of this policy using:

- logs of reported online safety incidents
- filtering and monitoring records
- internal network activity monitoring data
- surveys/questionnaires of learners, parents/carers and staff
- review of behaviour/bullying information and relevant safeguarding themes
- This policy will be developed and reviewed through a whole-school process drawing on the expertise of senior leaders, the DSL, Online Safety Lead, curriculum and technical staff, governors and, where appropriate, learners and parents/carers.
- The policy will be reviewed annually and sooner where there are significant technological developments, emerging risks, changes in national guidance or a serious incident.

3. Policy and leadership

Headteacher and senior leaders

- The Executive Headteacher and Head of School have a duty of care for the safety, including online safety, of members of the school community and for fostering a culture of safeguarding. Day-to-day lead responsibility for online safety sits with the Designated Safeguarding Lead (DSL).
- The Executive Headteacher, Head of School and senior leaders will know the procedures to follow where a serious online safety allegation is made against a member of staff.
- The Executive Headteacher and Head of School will ensure that the DSL/deputies, Online Safety Lead, IT provider/technical staff and other relevant staff can carry out their responsibilities effectively and receive suitable training.
- The Executive Headteacher and Head of School will ensure there is appropriate oversight and support for those who carry out internal online safety monitoring.
- Senior leaders will receive regular monitoring reports and will work with the responsible governor, DSL and IT provider on filtering and monitoring.
- Senior leaders will act on emerging themes and risks identified through incident, filtering, monitoring, curriculum and audit information.

Governors

- Governors are responsible for approving this Online Safety Policy and reviewing its effectiveness.
- The governing body will receive information about online safety incidents and monitoring through safeguarding/headteacher reporting.
- The safeguarding governor will take responsibility for online safety and will meet with the DSL/Online Safety Lead to review processes and procedures.
- The responsible governor will receive basic cyber-security awareness training and sufficient information to support oversight of DfE cyber-security and filtering/monitoring standards.

Designated Safeguarding Lead (DSL)

- The DSL holds lead responsibility for online safety within the safeguarding role.
- The DSL will receive relevant and regularly updated training so that they understand current online risks and the school's filtering and monitoring arrangements.
- The DSL will meet with the Safeguarding Governor (Online Safety Governor), review anonymised incidents and filtering/monitoring information, and ensure that filtering and monitoring checks are completed at least annually.
- The DSL will receive reports of online safety incidents, coordinate safeguarding responses, decide whether referrals are required, ensure incidents are recorded and liaise with relevant agencies.
- The DSL will liaise with staff and IT providers on safeguarding, welfare and online/digital safety.
- The DSL will ensure that online safety arrangements take account of learners with SEND and other vulnerabilities, including accessibility, communication needs and increased susceptibility to online harm.

Online Safety Lead / Digital Lead (if different from the DSL)

- Lead the Online Safety Group and work closely with the DSL on a day-to-day basis.
- Receive reports of online safety issues and ensure that relevant information is logged to inform future developments.
- Lead the establishment and review of online safety policies and associated documents.
- Promote awareness of and commitment to online safety education across the school.
- Work with curriculum leaders to ensure the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure staff know how to report online safety incidents and identify sources of training and advice.
- Liaise with technical, pastoral and support staff and maintain current knowledge of content, contact, conduct and commerce risks.

Curriculum Coordinator(s)

The relevant curriculum coordinator(s) will work with the DSL/Online Safety Lead to develop a planned and coordinated online safety education programme, using ProjectEVOLVE or an equivalent framework as appropriate. Provision may be delivered through Computing,

PSHE/RSE, other curriculum areas, assemblies and national initiatives such as Safer Internet Day and Anti-Bullying Week.

Teaching and support staff

- Understand that online safety is a core part of safeguarding and maintain awareness of current online safety matters and school practice.
- Read, understand and comply with the Staff Acceptable Use Agreement and relevant school policies.
- Use professional, school-approved systems for digital communication with learners and parents/carers.
- Immediately report suspected misuse or concerns through MPET's safeguarding reporting route [insert system/process].
- Embed online safety appropriately across learning, including research skills, copyright, plagiarism and critical evaluation of information.
- Supervise and monitor learner use of digital technologies and follow school procedures for personal devices, cameras, livestreaming and video-conferencing.
- Challenge online bullying, sexual harassment, discrimination and hateful behaviour and report concerns.
- Model safe, responsible and professional online behaviour, including in personal use of social media where this could affect the school.
- Follow data protection and cyber-security requirements.
- Complete online safety training at induction with additional training when risks, technology or responsibilities change.

IT service provider / technical staff

- Follow MPET's Online Safety and Technical Security requirements.
- Maintain secure infrastructure and managed user access.
- Support the school to meet relevant DfE digital and technology standards.
- Implement, maintain and update filtering and monitoring and provide reports to school leaders.

- Monitor systems for misuse and promptly report concerns.
- Keep technical knowledge current and support risk assessment, procurement and review.
- Where technical services are outsourced, MPET remains accountable for safeguarding and will ensure contractual providers understand and comply with the school's requirements.

Learners

- Use school digital systems in accordance with the Learner Acceptable Use Agreement *(see appendix)* and this policy.
- Report abuse, misuse, inappropriate material or anything that makes them or someone else feel unsafe or vulnerable.
- Respect copyright and intellectual property and avoid plagiarism.
- Use AI only as permitted, check the accuracy of AI-supported content and protect their own and others' work.
- Understand that out-of-school online behaviour may be addressed by the school where it affects members of the school community.

Parents and carers

Parents and carers play a crucial role in helping children use online services and devices safely and appropriately. MPET will support them through publication of this policy, learner AUAs, guidance, permissions where required, communications, events and national/local online safety campaigns. Parents/carers will be encouraged to reinforce school messages at home.

4. Online Safety Group

MPET will maintain an Online Safety Group or equivalent safeguarding/digital oversight group. Membership should reflect the school context and may include:

- DSL
- Online Safety/Digital Lead
- senior leader
- Online Safety Governor
- IT/technical representative

- curriculum representative
- teaching/support staff representative
- learner representative(s)
- parent/carer representative where appropriate

The group will support the DSL and Online Safety Lead by:

- reviewing and monitoring this policy and related documents
- reviewing filtering and monitoring arrangements and requests for change
- mapping and reviewing online safety education for relevance, breadth, progression and coverage
- reviewing anonymised incident, network, filtering and monitoring information to identify trends
- encouraging learner voice and consulting staff and parents/carers
- tracking improvement actions arising from self-review and audit

5. Policy and acceptable use

This policy sets expectations for the safe and responsible use of digital technologies for learning, administration and communication; allocates responsibilities; establishes reporting and response procedures; supports safe and professional staff practice; and helps learners become safe, responsible and critical users of technology.

Acceptable Use Agreements (AUAs) form part of the school's online safety framework. Their expectations will be reinforced through induction, education, reminders, communications with parents/carers and the school website. AUAs should be understood and followed, not treated simply as documents to be signed.

Unacceptable and illegal activity

- Child sexual abuse material, child sexual exploitation or grooming.
- Terrorism-related material or activity.
- Encouraging, promoting or assisting suicide or self-harm.

- Sexual image offences, including intimate image abuse and extreme pornography.
- Incitement to or threats of violence; hate crime; harassment or stalking.
- Drug-related, weapons/firearms, fraud or financial crime.
- Unauthorised access, password/account misuse, malware, disruption of networks or unauthorised penetration testing under the Computer Misuse Act 1990.
- Accessing inappropriate material in school, promoting discrimination, running a private business through school systems, bypassing safeguards, infringing copyright/intellectual property, unfair network usage, or sharing material that is offensive or brings the school into disrepute.
- Attempts to capture credentials through phishing or similar techniques, and the use of VPNs, proxies, anonymisers or alternative DNS to bypass school safeguards, are prohibited unless explicitly authorised for a legitimate technical purpose.

Communication technologies

- Professional communications must use technologies officially sanctioned by MPET.
- Digital communication between staff and learners or parents/carers must be professional in tone and content. Personal email, messaging and social media accounts must not be used for such communication.
- Users must report communications that are offensive, discriminatory, threatening, harassing or bullying and should not engage with them.
- Relevant policies and permissions must be followed when information is posted online.

Mobile phones and smart devices

MPET's rules for mobile phones, smartwatches, earbuds and other personal smart devices will be set out in the Behaviour Policy/Staff Code of Conduct and communicated clearly to learners, parents/carers, staff and visitors.

Under agreement with the class teacher and parent, children in Year 5 and Year 6 who walk unsupervised to or from school are permitted to bring a mobile phone, or for another valid reason. Learner devices brought to school with permission must be switched off before entering the school grounds and must not be turned back on until they have left school premises. Mobile phones will be stored in a locked safe within the Year 5 or Year 6 classroom.

6. Reporting and responding

MPET will take reasonable precautions to ensure online safety but recognises that incidents may occur in or outside school and may require intervention. The school will maintain clear reporting routes consistent with safeguarding, whistleblowing, complaints and managing allegations procedures.

- All members of the school community will be made aware of the need to report online safety issues and incidents.
- Reports will be dealt with as soon as reasonably practicable.
- The DSL, Online Safety Lead and relevant staff will have appropriate training.
- Where illegal activity or serious harm is suspected, the matter will be escalated through safeguarding procedures and external agencies will be involved as appropriate.
- Incidents, actions, decisions and follow-up will be recorded securely.
- Reporting routes will be accessible and inclusive and may include speaking to the DSL or another trusted adult.
- MPET will respond to anonymous or third-party reports where sufficient information is available to assess risk.
- People who report concerns will receive reassurance, appropriate support and, where appropriate and lawful, feedback about the outcome.
- Incident information will be audited and analysed to identify patterns, emerging risks and the effectiveness of responses. Anonymised themes will be shared with senior leaders, governors and other relevant groups.

Serious incidents and evidence

Where an incident may involve illegal content or activity, staff must prioritise immediate safeguarding, preserve evidence and follow police/DSL advice. Staff must not undertake their own investigation of suspected criminal material. Where indecent images of a child are suspected, staff must not intentionally view, copy or share the image.

- Where concerns do not involve suspected illegal activity, any examination of a device or online content will be lawful, proportionate, necessary and documented, and carried out only by authorised staff in line with MPET's Searching, Screening and Confiscation/Behaviour arrangements.

External support and escalation

Depending on the concern, MPET may seek support from or make referrals to the Local Authority safeguarding team, LADO, police/PCSO, the school's Data Protection Officer, the ICO, local safeguarding partners, the UK Safer Internet Centre Professionals Online Safety Helpline or other appropriate agencies.

7. School actions and sanctions

Responses will be proportionate, consistent and safeguarding-led. The school will distinguish between accidental, inappropriate, harmful and potentially illegal behaviour and will consider the age, needs, vulnerability and intent of those involved.

Responding to learner actions

- Educational response and reminder of expectations.
- Discussion with class teacher/Phase Lead/DSL.
- Contact with parents/carers where appropriate.
- Temporary restriction of access to devices, services or accounts.
- Technical action to protect systems or preserve evidence.
- Behaviour/safeguarding response in line with relevant policies.
- Referral to external agencies where required.

Responding to staff actions

- Concerns involving staff will be referred to the appropriate line manager, Headteacher and/or Trust/HR route as required.
- Allegations that meet safeguarding thresholds will be managed in accordance with the school's managing allegations procedures and referred to the LADO/police where appropriate.
- Technical support may be asked to secure systems, preserve logs or change access.
- Breaches may lead to disciplinary action in line with employment procedures.

8. Use of Artificial Intelligence (AI)

MPET recognises that generative AI can support learning, teaching and administration, while introducing risks relating to safeguarding, privacy, security, accuracy, bias, intellectual property and academic integrity. AI must be used safely, ethically and responsibly.

- Only school-approved AI services and accounts may be used for school purposes.
- Staff remain professionally responsible and accountable for work supported by AI. AI may assist but must not replace human professional judgement, particularly in decisions affecting people.
- AI outputs must be critically evaluated and fact-checked for accuracy, bias and suitability.
- Personal or sensitive data must not be entered into AI systems unless the system and purpose have been explicitly approved and data protection requirements have been satisfied.
- Copyright and intellectual property must be respected. Learners' or staff work must not be used to train AI systems without an appropriate lawful basis/consent where required.
- AI-related incidents, inappropriate outputs, data breaches or suspected misuse must be reported promptly.
- Learners will be taught about the safe, ethical and effective use of AI, including limitations, misinformation, bias, attribution and plagiarism.
- Procurement and implementation of AI systems will consider fairness, security, privacy, age appropriateness, supplier terms, data use/training practices and the potential for discrimination or bias.
- MPET will provide staff training on AI and will support parents/carers to understand how AI is used in school and the risks and expectations associated with its use.
- AI must not be used to impersonate others, create deceptive or harmful content, or generate/manipulate sexualised or abusive images.

9. Online Safety Education Programme

Online safety education will be planned, progressive and regularly reviewed. It will be embedded across appropriate curriculum areas and reinforced through assemblies, pastoral provision and national initiatives.

- Learners will be helped to understand content, contact, conduct and commerce risks.

- Teaching will cover privacy, personal information, passwords, online relationships, bullying, harmful content, misinformation, scams, copyright, AI, digital reputation and how to report concerns.
- Learners will be taught research and information literacy skills, including checking reliability, recognising bias and understanding how search, recommendation and AI systems can influence what they see.
- Education will promote respectful, responsible and ethical online behaviour and healthy, balanced use of technology.
- Provision will be adapted for age, developmental stage, SEND, vulnerability and accessibility needs so that all learners can understand risks, reporting routes and protective strategies.
- The school will evaluate the impact of online safety education using curriculum review, pupil voice, incident themes and other evidence, and will adjust provision accordingly.

10. Staff, governors, parents/carers and external stakeholders

Staff and volunteers

Online safety training will be included in safeguarding induction and updated regularly. Staff will receive additional information or training where technology, risks or responsibilities change.

Governors

Governors will receive online safety awareness training appropriate to their oversight role. The Online Safety Governor will receive enhanced training on filtering/monitoring and cyber security.

Working with parents and carers

MPET will provide communication, awareness raising and opportunities for engagement on online safety, curriculum content and reporting routes. Learners may also contribute to parent/carer awareness activity.

Wider community and agencies

MPET will work with external stakeholders and agencies where this strengthens prevention, education, safeguarding or incident response. Relevant partners may include the Local Authority, safeguarding partnership, police/PCSO, health or early-help services, the DPO, technical providers and specialist online safety organisations.

Visitors, contractors and community users who access school systems will be informed of relevant expectations and, where appropriate, required to accept a Community User AUA.

11. Technology

MPET is responsible for ensuring that its infrastructure and network are as safe and secure as reasonably possible and that agreed policies and procedures are implemented. All users share responsibility for online safety, data protection and cyber security.

The school will ensure that technology is procured, configured and managed with safeguarding, privacy and security in mind and that access is appropriate to users' roles and needs.

12. Filtering and monitoring

Filtering and monitoring arrangements will be agreed by senior leaders, governors and the IT service provider and reviewed at least annually, and sooner where technology, risk or patterns of behaviour change. The DSL has lead safeguarding responsibility and the IT provider has technical responsibility.

Filtering

- MPET will manage access to online content across school systems and devices using filtering that meets relevant DfE standards.

- Illegal content will be blocked using appropriate provider lists and mechanisms, including relevant IWF (Internet Watch Foundation) and unlawful terrorism content lists where applicable.
- Users will have clear routes to report inappropriate content because no filtering system can be completely effective.
- Requests to change filtering will be authorised, recorded and reviewed.
- Filtering will be age-appropriate, proportionate and designed to avoid unreasonable over-blocking that would restrict teaching and learning.

Monitoring

- MPET will use monitoring arrangements appropriate to its context and risk profile.
- Monitoring alerts and reports will be reviewed by appropriately trained staff and escalated according to safeguarding procedures.
- Access to monitoring information will be controlled and privacy will be respected.
- Monitoring arrangements will be tested and reviewed to ensure they are effective.

13. Technical and cyber security

- Users will have individual accounts and must keep passwords secure.
- Administrative privileges will be restricted and managed.
- Systems, devices and software will be patched and updated appropriately.
- Malware protection, backup and recovery arrangements will be maintained.
- Network and system logs will be retained and reviewed as appropriate.
- Remote access and cloud services will be approved and secured.
- Cyber incidents will be reported promptly and managed through the school's incident response/business continuity arrangements.
- Staff and governors will receive training on common cyber threats and learners will receive age-appropriate cyber awareness education.
- MPET will maintain and test business continuity and cyber incident response arrangements, including restoration from backups and communication/escalation routes.

14. Data protection

MPET is committed to protecting personal data and complying with UK data protection legislation. Personal data will be processed lawfully, fairly and transparently, collected for specified purposes, limited to what is necessary, kept accurate, retained only as long as needed and protected by appropriate security.

- A Data Protection Officer (DPO) will be appointed and appropriate governance arrangements maintained.
- Privacy notices will explain how personal data is used and how rights can be exercised.
- Personal data will be stored, shared, transferred and disposed of securely.
- Staff will receive data protection training at induction and appropriate refresher training.
- Data breaches will be reported and managed promptly in accordance with legal requirements.
- School personal data must not be transferred to personal devices or unapproved services.
- Data Protection Impact Assessments (DPIAs) will be considered and completed where required for existing or planned software, systems and processing that is likely to create high risk to individuals.
- MPET will maintain procedures for Subject Access Requests and other data subject rights, and will notify the ICO within statutory timescales where a reportable personal data breach occurs.

15. Technology practice and device management

MPET will define and communicate expectations for school-owned and personal devices, including laptops, tablets, phones, cameras, removable media and other connected devices.

- Device use will be consistent with safeguarding, behaviour, data protection and acceptable use requirements.
- School devices will be configured and managed using appropriate technical controls.
- Staff, learners and visitors will understand their responsibilities when using devices on school premises or systems.
- Safe and responsible device use will form part of online safety education.
- Loss, theft, damage or suspected compromise of a school device must be reported promptly.

Searching, screening and confiscation of electronic devices

Any search, examination, confiscation or deletion of data from a learner's electronic device will be carried out only where lawful, proportionate and necessary, by authorised staff and in accordance with the Behaviour Policy and current DfE guidance. Criminal material will be referred to the police and potential evidence will not be deleted.

16. Digital content, images and video

Digital images, video, audio and other digital content can enrich learning and communication but may create safeguarding, privacy and reputational risks. MPET will educate users about the safe creation, use, storage, sharing and publication of digital content.

- Staff will use school devices for images/video of learners unless an alternative has been explicitly approved.
- Staff and volunteers must know which learners' images may not be taken or published.
- Consent and privacy requirements will be followed.
- Learners must not take, use, share or publish images of others without permission.
- Published images will be selected carefully and learners will not be unnecessarily identified.
- Content will be stored and shared securely and removed where consent is withdrawn when required.
- MPET will consider the risk of AI-enabled manipulation, deepfakes and other misuse of publicly available images. Publication practices will minimise unnecessary exposure of identifiable images of learners and staff.
- Education will address consent, coercion, sexual imagery, image-based abuse and the risks of creating or sharing manipulated or synthetic media.

17. Public online communications and social media

MPET may use its website, newsletters, learning platforms, public messaging systems and official social media accounts to communicate with the community. Public communications must be professional, respectful, lawful and consistent with safeguarding and data protection.

- Official accounts may only be created with senior leadership approval.
- At least two authorised staff members should have access to official public accounts where practicable.
- Accounts will be securely administered, monitored and moderated.
- Personal information and confidential/sensitive information will not be published inappropriately.
- Staff must not engage with current learners through personal social media accounts.
- Where personal accounts refer to or affect the school, staff must maintain professional standards and make clear that personal views are not expressed on behalf of MPET.
- Parents/carers raising complaints through social media will be directed to the school's formal complaints process.
- Serious online abuse or threats will be recorded and escalated as appropriate.
- Staff responsible for public accounts will receive appropriate guidance/training
- Public communications will be monitored regularly; harmful or inappropriate comments/content will be moderated or removed where the school controls the platform, and serious incidents will be recorded and escalated.

18. Outcomes

The impact of this policy and associated practice will be evaluated through review of incident logs, behaviour/bullying information, filtering and monitoring data, curriculum review, surveys and stakeholder feedback.

- Online safety issues are identified and addressed promptly.
- Learners understand how to use technology safely, responsibly and critically and know how to seek help.
- Staff understand their safeguarding, professional, data protection and cyber-security responsibilities.
- Parents/carers understand key risks and know how to report concerns.
- Filtering, monitoring and technical controls are proportionate and effective.
- Governors receive sufficient evidence to challenge and assure the school's arrangements.
- Evaluation will focus on impact and improvement, with identified actions assigned, monitored and reported through the school's safeguarding/governance arrangements.

19. Related policies and appendices

This policy should be read alongside MPET's relevant policies and procedures, including:

- Safeguarding / Child Protection Policy
- Relationship and Behaviour Policy
- Staff Code of Conduct
- Data Protection / Data Security Policy
- Filtering and Monitoring Policy
- Complaints Policy
- Whistleblowing Policy
- Acceptable Use Agreements

Appendix – KS2 Learner Acceptable Use Agreement

Our Technology Rules

I agree to use Mulberry Park Educate Together's digital systems safely and responsibly to protect me, other learners and the school.

Keeping safe online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed and if they have given consent
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.

Using devices and the internet sensibly

- I will only use devices, apps and sites I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being respectful and responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What happens If I don't follow the rules

- If I don't follow these rules, an adult at MPET may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Child's name: Class:

Signed:

Date:

Parent/Carer countersignature :

Appendix EYFS/KS1 Learner Acceptable Use Agreement

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at MPET.

Staying safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I will not share my name, address, or pictures without asking a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using technology kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making good choices

- I will ask my teacher before I use someone else's pictures or work.
- I know that I can say "no" /" please stop" to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What happens if I don't follow the rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Child's name: Class:

Date: Parent/Carer countersignature :