E-Safety, Online Safety and Social Media Policy

Policy Statement

Manor Farm Fun Ltd recognises that digital technology and online communication are an important part of everyday life and learning. We are committed to ensuring that children, young people and staff can use technology safely, responsibly and appropriately.

Online safety is an integral part of safeguarding. We recognise that children and young people may have differing levels of understanding, communication, emotional regulation and awareness of online risks. Support and teaching will therefore be developmentally appropriate and responsive to individual needs.

This policy applies to all staff, children, young people, volunteers, visitors and anyone using Manor Farm's digital systems or accessing online services on its behalf.

Legal and Guidance Framework

This policy has regard to relevant legislation and statutory guidance, including:

- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025.
- Children Acts 1989 and 2004.
- Equality Act 2010.
- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Online Safety Act 2023.
- Counter-Terrorism and Security Act 2015 and relevant Prevent guidance.
- Keeping Children Safe in Education and Working Together to Safeguard Children, where applicable.
- Department for Education filtering and monitoring guidance.
- UKCIS Education for a Connected World.
- Department for Education guidance on sharing nudes and semi-nudes.

This policy should be read alongside the Safeguarding and Child Protection Policy, Staff Code of Conduct, Acceptable Use arrangements, GDPR and Privacy Policy and Mobile Phones, Devices and Cameras Policy.

Roles and Responsibilities

Leadership Team

Our senior leadership team consists of Hannah O'Brien, Daisy Bowden and Sarah Powell.

- Ensure appropriate systems, policies and procedures are in place and abided to throughout day-to-day operations.
- Provide oversight of online safety and safeguarding arrangements.
- Ensure staff receive appropriate training.

Designated Safeguarding Lead (DSL)

Manor Farm's DSL is Noah Denman.

- Lead the response to online safeguarding concerns.
- Refer concerns to children's social care, police or other agencies where appropriate.
- Ensure online incidents are recorded and managed in accordance with safeguarding procedures.

IT Manager

Manor Farm's IT Manager is Daniel O'Brien.

- Oversee the technical security of systems, including filtering, monitoring, access controls and software.
- Support the investigation and management of technical incidents.
- Ensure new software and applications are considered through the New Software or App Request procedure.

All staff

- Model safe and responsible technology use.
- Follow this policy and report concerns promptly.
- Maintain professional boundaries when communicating online.
- Support children and young people to develop safe online behaviours.

IT Systems, Filtering and Monitoring

Manor Farm uses managed internet filtering and security measures through Microsoft and Apple Education services to help protect users from inappropriate or harmful online content.

Systems include secured physical and wireless networks, separate guest Wi-Fi and virus protection on compatible devices.

Filtering and monitoring arrangements will be reviewed regularly to ensure they remain effective and appropriate. The Leadership Team, DSL and IT Manager will work together to identify and respond to concerns.

Staff must not attempt to bypass filtering or security arrangements. Any technical weaknesses, inappropriate content or suspected breaches must be reported to the IT Manager and, where safeguarding is involved, the DSL.

New software, applications and online platforms must be approved through our bespoke New Software or App Request procedure before use.

Acceptable Use and Staff Responsibilities

All staff are expected to:

- Use Manor Farm systems for appropriate professional purposes.
- Keep passwords secure and never share login details.
- Access only information and systems necessary for their role.
- Protect confidential information and personal data.
- Avoid accessing, creating or sharing inappropriate material.
- Report suspicious emails, links, downloads, cyberbullying or other online concerns.
- Ensure children are appropriately supported and supervised when using technology.

Personal devices and mobile phones must be used in accordance with the separate Mobile Phones, Devices and Cameras Policy. Staff must not use personal social media or private messaging accounts to communicate with children or young people.

Children's and Young People's Online Safety

Children and young people will be supported to use technology safely and responsibly. Online safety education will be incorporated into relevant learning and safeguarding activities, taking account of individual developmental needs.

This will include:

- Protecting personal information, passwords and privacy.
- Recognising inappropriate contact, grooming and exploitation.
- Understanding cyberbullying and how to report it.
- Safe use of social media, gaming and online communication.
- Understanding consent and the risks of sharing images.
- Recognising scams, misinformation and harmful content.
- Understanding digital footprints and online reputation.
- Knowing how to seek help when something online causes concern.

Staff should provide appropriate supervision and support, particularly where a child or young person may be vulnerable to online manipulation, exploitation or harmful content.

Social Media and Professional Boundaries

Staff must maintain appropriate professional boundaries when using social media and online communication.

Staff must not:

- Initiate or accept personal social media connections with current children or young people.
- Communicate with children through personal accounts, private messaging or personal email. Manor Farm has separate Post-16 and Staff Mobile Communication Policy detailing acceptable communication with post-16 students.
- Share identifiable information, photographs or videos of children without appropriate authorisation.
- Post confidential information or comments that could bring Manor Farm, its children, families or staff into disrepute.

- Use social media to discuss individual children, families or safeguarding matters.
- Approved organisational communication channels, including relevant Tapestry accounts, must be used where appropriate. Concerns about inappropriate online contact, impersonation, harassment or breaches of professional boundaries must be reported to the Leadership Team or DSL.

Email and Online Communication

Staff must use approved work email accounts and communication platforms for professional purposes. Sensitive or confidential information must be shared securely, using Egress where appropriate.

Children's Wickslem pupil email accounts and access to online communication must be appropriately managed and supervised.

Video conferencing platforms, including Zoom and Microsoft Teams, must be approved for use. Staff should:

- Use professional accounts and approved meeting links.
- Check privacy settings and participants.
- Ensure children are appropriately supported.
- Avoid recording meetings unless there is an authorised and legitimate reason, ensuring all parties have provided consent.
- Store any authorised recordings securely and in accordance with data protection requirements.

Cyber Security, Personal Data and Artificial Intelligence

Manor Farm will take reasonable steps to protect its systems and information through appropriate access controls, passwords, security software, updates and secure information-handling procedures.

Personal data must be collected, accessed, stored and shared in accordance with the Data Protection Policy, UK GDPR and Data Protection Act 2018, as amended. Subject Access Requests (SAR) for access to personal data will be managed in accordance with statutory timescales, within one calendar month, subject to any lawful extension or exemption.

Staff must not enter identifiable, confidential or sensitive information about children, families or colleagues into unapproved online tools or artificial intelligence (AI) platforms. AI-generated information must be checked for accuracy, bias and appropriateness. AI must not replace professional judgement, safeguarding decisions or individual assessment. Please refer to our Artificial Intelligence (AI) Use Policy.

Suspected data breaches, phishing attempts, malware or other cyber security incidents must be reported immediately to the IT Manager and Leadership Team, with safeguarding concerns also referred to the DSL.

Copyright and Intellectual Property

Staff and children must respect copyright and intellectual property when accessing, downloading, copying or sharing digital material.

The Copyright, Designs and Patents Act 1988 provides limited exceptions, including certain fair dealing provisions for education. These exceptions have conditions and do not provide unrestricted permission to copy or distribute material.

Online Safeguarding Concerns and Incidents

Any concern involving online abuse, grooming, exploitation, cyberbullying, inappropriate communication, harmful content or unsafe use of technology must be reported promptly to the DSL.

Any E-safety concerns are logged and dated by the DSL, IT Manager or the Leadership Team. Any action taken will be recorded on CPOMs. This includes information about the nature of the incident, who was involved and how it was dealt with. If the incident is of an illegal nature, the PC should be disconnected from the mains without shutting down first and the police and Local Authority Designated officer (LADO) informed. The log is reviewed to identify any trends and issues that may need addressing.

Sharing of nude or semi-nude images

Any incident involving the creation, receipt or sharing of nude or semi-nude images involving a child or young person must be reported immediately to the DSL. Staff must not view, download, copy, screenshot, forward or distribute such images, or investigate independently. The DSL will manage the response in accordance with safeguarding procedures and current Department for Education guidance.

Where an allegation or concern relates to an adult working with children, the appropriate safeguarding and allegations procedures must be followed, including referral to the Local Authority Designated Officer (LADO) where the relevant threshold is met.

Where an incident may involve a criminal offence, the DSL or appropriate senior leader will seek advice from the police or relevant safeguarding agencies. Staff must preserve any relevant information and avoid taking action that could compromise potential evidence. Where appropriate, disciplinary procedures will be followed to address any misconduct and ensure the ongoing safety and protection of children, young people and staff.

Preventing Online Radicalisation

Staff should remain alert to online content or contact that may expose children and young people to extremist or radicalising influences. Any concern must be reported to the DSL and managed in accordance with safeguarding and Prevent procedures.

Training, Reporting and Review

Staff will receive appropriate online safety and safeguarding training, including guidance on recognising and reporting online risks. Online safety will be reinforced through ongoing staff discussions and developmentally appropriate learning for children and young people.

All online safety concerns must be reported to the DSL or Leadership Team without delay and recorded in accordance with safeguarding procedures on CPOMs.

This policy will be reviewed at least annually, or sooner where there are significant changes to legislation, statutory guidance, technology or safeguarding practice.

Policy Last Reviewed: 10th November 2026

Next Review Due: 10th November 2027