**E-Safety Policy, Including Social Media**

**Online-Safety**

Internet use is now an essential aspect of life, it pervades every activity that we undertake and is increasing its hold. It is part of our curriculum and is a necessary tool for staff and children. By design, it is insecure. Everyone in the Manor Farm community has a personal responsibility to work towards keeping themselves and others safe online.

**Infrastructure**

* All aspects of the setting’s IT systems are managed and reviewed by the IT Manager, Hannah O’Brien.
* Internet access is a managed filtered service. Virus protection is installed on all compatible devices and updated regularly.
* Security strategies will be periodically discussed between the IT Manager and Leadership Team.
* Physical and Wi-Fi networks are secured – for instance through password protection
* A separated Guest network is in place for any visitors using IT on site

**Filtering**

All internet access within the setting is filtered through the use of standard filtering policies. These are designed specifically with the safety of children in mind.

Where access to a specific website is required by staff but not children, the website is un-filtered via the custom filtering policies and then filtered through our internal proxy server.

The IT Manager, will be responsible for conducting online safety audits on a termly basis.

**Staff Responsibilities**

The IT Manager regularly monitors internet access and brings any issues to the attention of the rest of the Leadership team who then take appropriate actions. This includes spot checking iPads for inappropriate content.

The IT Manager will undertake regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Staff will protect the setting from computer virus attack or technical disruption by not downloading from the internet any programs or executable files other than by agreement with the setting’s IT Manager.

Staff will not purchase goods or direct services over the internet other than when specifically requested to do so by the setting lead.

All staff using technology within setting should have appropriate content only and be aware that internet usage and technology devices’ content will be monitored.

Staff using the setting technology (for example laptop/ iPad) off site, at home or elsewhere, still have to abide by this policy and the staff Acceptable Use Policy.

Colleagues will be aware that the misuse of such devices for activity not agreed by the setting may be breaking the law under the computer misuse Act 1990.

All staff should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet, see below:

**Copyright law for internet downloads and copying:**

Copyright is a law that protects the creator’s right to control how their work (like music, movies, books, software, or photos) is used and shared.

**Downloading Content:**

**Legal:** Downloading content is legal if you have permission, like buying music from iTunes or downloading free content from a legitimate source.

**Illegal:** Downloading copyrighted material (e.g., movies, music, software) from unauthorized websites or torrents without paying or getting permission is usually illegal.

**Copying Content:**

**Fair Use:** Some copying is allowed for purposes like education, commentary, or research, but it has limits. For example, quoting a short passage from a book for a school project is often okay.

**Infringement:** Making full copies or distributing someone else’s work without permission (e.g., uploading a movie to YouTube) is illegal unless the work is in the public domain or under a license like Creative Commons.

**Streaming vs. Downloading:**

Streaming (watching/listening without downloading) from unauthorised sources can still be illegal, but enforcement may focus more on the site owners than users.

Downloading from unauthorised sources creates a permanent copy, making it more likely to be a copyright violation.

**Consequences:**

Copyright infringement can lead to fines, lawsuits, or takedown notices. However, enforcement varies depending on where you live.

Rule of Thumb: If you didn’t create it or pay for it legally, assume you need permission to download or copy it. Stick to licensed or legal sources.

**Misuse and complaints**

Any E-safety issues are logged and dated by the IT Manager and the Leadership Team. Any action taken will be recorded. 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.

If staff or children discover an unsuitable site, it will be reported to the IT Manager who will immediately ensure the website is filtered out and reported.

Complaints of internet misuse will be dealt with by a member of the Leadership Team and any complaint about staff misuse will be referred to the setting lead in accordance with the setting staff disciplinary procedures.

Login passwords must not be shared with anyone. Users are provided with their own login passwords which can be used to monitor any action taken when logged on and every user is responsible for the action taken while their username is in use.

Children’s technology devices will be closely monitored and spot checked to ensure they are accessing appropriate content.

**Managing Internet Access**

Children will be monitored when carrying out internet searches to ensure that they are accessing safe and appropriate material.

Children will be directly supervised when accessing specific approved online material.

The setting will take all reasonable precautions to ensure that users access appropriate material. However, it is not possible to guarantee that unsuitable materials will never appear on the setting technology, but action will be taken to prevent misuse or unsuitable access to content from happening again.

**Training**

The IT Manager will attend regular training in order to keep up to date with the latest recommendations and filter back to staff.

There will be regular staff training regarding e-safety to ensure we are minimising potential risks.

The setting will communicate, support and advise parents in matters of e-safety, ensuring relevant information is being shared.

All staff should acknowledge that they have read this policy.

**Electronic Communications (e-mail)**

Children will only use approved e-mail on the setting’s system.

Children will be supported using e-mail. Offensive e-mails should be reported straight away to managers/ safeguarding lead or members of the Senior Leadership team. All childrens’ e-mails will be treated as public.

Children must not reveal personal details of themselves or others in any online communication.

Staff e-mails to outside organisations should be written using a professional voice (the same way as a letter would be written).

Staff emails containing personal sensitive data should be sent confidentially using ‘Egress’ when sending to outside agencies.

Manor Farm staff mobile phones are an acceptable form of communication across our large outdoor site and should be used as a means to summon assistance in emergencies. For further information regarding acceptable phone usage, please also see our Use of Mobile Phones, Devices and Cameras Policy.

**Social Networking / Social Media**

Manor Farm will block/ filter access to open social networking sites and will only give access to sites that are monitored and approved.

Tools including message boards, blogs and instant messaging will be used in safer, controlled learning sites which have been approved.

Children will be taught about the potential risks of social networking sites and what information should and should not be shared on these sites.

Staff should not provide information of their own, or another person/ child’s that could relate to Manor Farm to any internet sites including all social media websites. Exceptions should be checked with the manager.

Staff should not post any derogatory comments on social media relating to Manor Farm, any of its employees, children, families or anyone who represents the organisation. Failure to comply will result in disciplinary action.

**Protecting personal data**

Personal data will be recorded, processed and transferred, and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2015.

**Acceptable use of Video Conferencing/ Skype**

A log will be kept of all video conference calls (including date, time, whom with and who else was present).

Children must always be supervised by a member of staff when video conferencing.

Unsuitable content must be reported to the Designated Safeguarding Lead immediately.

**Reporting**

Incident Reporting – should anyone breach these policies for whatever reason, they should report it to a member of the Leadership Team. If others are seen or suspected of operating in breach of these policies, they must report it immediately to the Designated Safeguard Lead, the Deputy Designated Safeguarding Lead or Leadership Team.