ICT Safe Use and Social Media Policy Document

Introduction

Safeguarding is a serious matter. At Manor Farm Infant School, we use technology and the internet as a discrete subject and across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and so it is crucial that staff and families stay vigilant to protect pupils and staff from harm while using internet technology.

We aim to:

- Ensure the requirement to empower the whole school community with the knowledge to stay say and risk free is met.
- Ensure that risks are identified, assured and mitigated (wherever possible) in order to reduce any foreseeability of harm to the student, staff member or liability to the school.

A copy of this policy and School Home agreement document are distributed to parents upon first entry to the school. Upon return of the signed Home Agreement, which will be taken as an acceptance of the school's terms and conditions, children will be allowed to use school technology and the internet in line with our Computing Curriculum policy.

Headteacher

The Headteacher has overall responsibility for safety within our school and reports to the Governing Body. The day-to-day management of this will be delegated to the Designated Safeguarding Leads, Computing Coordinator and/or Teams as indicated below.

Manor Farm Infant School will ensure that:

- E-safety training throughout the school is planned, up to date and appropriate to the recipient ie. Pupils, all staff, senior leadership team (SLT), governing body, parents.
- The Designated and Deputy Designated Lead for Safeguarding has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

The Safeguarding Team will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review policies regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, SLT and the governing body on all e-safety matters.
- Engage with parents and the school community on safety matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for logging e-safety incidents, ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school eg. internet filtering software are fit for purpose through liaison with the local authority and/or IT technical support.
- Make themselves aware of any reporting function with the technical e-safety measures ie. internet filtering reporting functions; liaise with the Headteacher and/or governing body to decide on what may be appropriate for viewing.

ICT Technical Support Staff (Third Party Provider)

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure. This will include, as a minimum:

- Antivirus software that is fit for purpose, up to date and applied to all devices.
- Operating system updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions are operating correctly. Ie. Internet filtering.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Designated Person for Child Protection and Headteacher.
- Passwords are applied correctly to all users regardless of age.
- The IT System Administrator password is to be change on a minimum of a termly basis or at notification of a breach whoever is sooner.
- Password protection of all laptops, tables, desktop computers.
- Encryption of all files that contain sensitive or other restricted information, including the secure data G: network drive.

All Staff

Staff are to ensure that:

- All details within this policy are personally understood. If anything is not understood then it should be brought to the attention of the Headteacher or the Designated Safeguarding Leaders.
- Any e-safety incident is reported to the Designated Safeguarding Leaders or a member of the Safeguarding Team.

Pupils

The boundaries of the use of computing equipment and services in this school are given in the Home School Agreement and the Internet Code of Practice. Deviation of misuse of computing equipment or services will be dealt with in accordance with our Behaviour Policy.

E-Safety is embedded into our curriculum students will be given the appropriate advice and guidance by staff. Similarly, all pupils will be aware how they can report concerns whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children. The school will work with parents to enhance the skills and knowledge they need to protect children outside the school environment.

Through information evenings, school newsletters and email communication, the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the strategies that the school must have in place to ensure that their child can be properly safeguarded. As such, parents need to sign the pupil Internet Code of Practice before access can be granted to school computing equipment or services.

Digital media, such as photos and videos, are covered in our Home School Agreement. All parents must sign a photo release form at the beginning of each academic year; non-return of the form will not be assumed as acceptance.

During school performances, parents/carers are permitted to take photos of their children only. It is not acceptable at any time to upload any photos, videos or comments that include other children at school on to any form of social media as this is a safeguarding risk.

Parents should not use their mobile phones (unless in case of emergency) and social media should not be accessed while helping at school or on school visits. Whilst helping or on a school visit, photos should not be taken on mobile phones or personal cameras.

Technology

Manor Farm Infant School use a range of devices, including desktop computers, laptops and tablets. In order to safeguard pupils, staff and prevent loss of personal data, we employ the following

- **Internet Filtering** – The local authority operates filtering software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites**.** Appropriate and inappropriate websites are determined by the age of the user and will be reviewed in line with this policy or in response to an incident - whichever happens sooner. The Third Party Provider and the Safeguarding Team are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher or Designated Safeguarding Leaders as appropriate**.**
- **Email filtering –** Email filtering is in place to prevent any infected email being sent to and from the school. This includes emails that contains a virus or script (ie. Malware) that could damage or destroy data, and spam emails such as a phishing message.

- **Passwords –** All staff and pupils will be unable to access any device without a unique username and password. Staff passwords are strong and robust. They should be changed termly (The Third Party Provider ensures this) and must be changed if there has been a compromise. Any terminals not in use must be logged off or locked in order to prevent misuse.
- **Encryption** – All school devices that hold personal data (as defined by GDPR) are encrypted. No data about the school is to be kept on an unencrypted device. All devices that are kept on school property and which may contain personal data are encrypted. Any breach, such as loss/theft of a device, including laptops and USB sticks, is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to determine the action be to taken. **Note –** encryption is different to password protected.
- **Anti-virus –** All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The Third Party Provider will take responsibility for this task and report to the Headteacher if there are any concerns.

Safe Use

- **Internet –** Use of the internet in school is a privilege, not a right. Internet use will be granted to pupils upon signing the Home School agreement. Staff will also sign an Acceptable Use Policy.
- **Emails –** All staff are reminded that emails are subject to Freedom of Information requests and Subject Access Requests, and so the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes are not permitted. If staff are communicating with parents via email, this is advised to go through the office's administrator account. Students will be given access to a school email address for the purposes of remote learning.
- **Social Media –** It is against school advice to "befriend" or "follow" parents on Social Media. Staff are advised to change their privacy settings to "private" or "friends only" to safeguard themselves.
- **Photos and videos -** All photos and videos that are taken within school or school trips must only be taken on school cameras or iPads and stored on these devices or on our school network. It is not acceptable to use personal devices to take photographs of the children or school setting.
- **Child Identity –** Permission slips must be consulted before any images or video of ay child is uploaded to the school website. The child's surname will never be used to identify the child; just their first name.
- **Copyright Law** – All posted data must conform to copyright law; images, videos and other resources hat are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence that allows such use.

- **Notice and take down policy –** In the event where a resource that has been uploaded to the school website or internal network that breaches copyright or is inappropriate, it will be removed within one working day.
- **Incidents –** Any e-safety incident is to be brought to the immediate attention of the Safeguarding team, Headteacher or Designated Safeguard Leaders. The will take the appropriate action to deal with the incident and complete an incident log.
- **Training and Curriculum –** It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible while using digital technology. This includes updated awareness of new and emerging issues. School will provide regular training for pupils, staff, parents and carers. We will also establish further training in response to any e-safety incidents.
- **E-Safety –** E-safety for students is embedded into the curriculum. Staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Staff will also be available to address any questions or concerns raised by the pupils.
- **E-Safety Officer –** The E-Safety Officer is responsible for recommending a programme of training and awareness to the Headteacher and Governing Body for consideration and planning. Should any staff member feel they have had inadequate or insufficient training and/or experience in a particular area this must be brought to the attention of the Headteacher or Senior Leadership Team.

Software

Only licensed software may be installed onto school laptops and computers. Currently installed software includes: Microsoft Edge, Google Chrome, iTunes, Microsoft Office and 365. Staff and pupils are not authorised to install unlicensed software on school computers or laptops. If a member of staff requires special or non-standard software to be installed for school use, it must be cleared by the Network Manager and/or Third Party Person beforehand. The member of staff will be responsible for supplying the licenses, media and any documentation. License information is a requirement for the County Auditors.

Software used is school is licensed in a correct and legal manner. However, I is no available to users for home usage unless accessed through the school VPN (for staff only). Users should make no attempt to copy licensed or copyrighted materials from the school network.

Users may not download copyrighted software, audio or video files, or ay other copyrighted material from the Internet. Any such material found will be deleted without prior notification.

Breach of any of these conditions may lead to disciplinary action.

Networking

For network connection of computers, users are provided with a dedicated account. The user is to use no other account on the network. The use should always keep their passwords for their account secure and private. The user takes full responsibility for the use and misuse of this account.

This account allows the user certain privileges and rights on the network. The user should in no way attempt to gain other privileges to attempt to access resources on the network to which no explicit rights have been granted.

The user shall not, in any way, tamper with or misuse school equipment – either software or hardware.

Computers and devices can have access to the internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious beach of the law (Child Trafficking and Pornography Act 1998). The school will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.

General:

The facilities are for school related educational use only. The facilities are not available for use on external projects or for work activities not associated directly with the school. Facilities may no be used for any form of personal financial gain.

The contents of all mailboxes, PCs. Server shares and caches operated by the School remain the property of the school. The status of these data stores is similar to that of letters posted to the school to a post holder (not marked as personal and private).

Email should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally, it should be done so in an encrypted form. Although every effort is made to ensure that home folders ad emails are secure, the School does not in any way guarantee the security of this data.

Social Networking

We understand that social networking sites and blogging are extremely popular. Users must not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

Basic Security

All users must protect the access and integrity of computing and information technology sources.

For example, it is a violation to: release a virus or worm that damages or harms a system or network to prevent others from accessing an authorised service; send email bombs that may cause problems and disrupt services for other users; to deliberately degrade, perform or deny service; to corrupt or misuse information; to alter or destroy information with authorisation.

General Usage

Food and drinks should be kept well away from computers. The user use should take care when shutting down and closing the lid of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case he user will be liable for the repair costs.

Authorisation

Use only those computing and information technology resources for which you have authorisation.

For example, it is a violation to: use resources you have not been specifically authorised to use; to use someone else's account ad password; to share your account and password with someone else; to access files, data or processes without authorisation; to purposely look for or exploit security flaws to gain system or data access.

Intended Use

Use computing and information technology resources only for their intended purpose.

For example, it is a violation to: send forged email to misuse networking, Internet Relay Chat (IRC) Instant messaging software to allow users to hide their identity; to interfere with other systems; to use electronic resources for harassment or stalking other individuals; to send bomb threats or hoax messages; to send chain letters; to intercept or monitor any network communications not intended for you; to use computing or network resources for advertising or other commercial purposes; to attempt to circumvent security mechanisms.

Law

Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, included the legal use of copyrighted software.

For example, it is a violation to; make more copies of licensed software than the license allows to download; to use or distribute pirated software; to operate or participate in pyramid schemes; to distribute pornography to minors; to upload, download, distribute or possess child pornography.

Privacy

Respect the privacy and personal rights of others.

For example, it is a violation to: tap a phone line or run a network sniffer without authorisation; to access or attempt to access another individual's password or data without explicit authorisation; to access or copy another user's electronic mail, data, programmes or other files without permission.

Date approved: November 2023

Review Date: November 2024