MANOR LEAS INFANT SCHOOL

Learning for Life

ICT Acceptable Use

(including mobile technology)

Policy number	91
Policy revision	5
Policy reviewed	Summer 2026
Review date	Summer 2027
Committee	FB
Authors	Headteacher

Mobile Technology Policy for Manor Leas Infant School

1. Aims of this policy

- To set out individual responsibilities which assist Manor Leas Infant School (the school) in protecting its Information and Communication Technology (ICT).
- To inform staff of their general responsibilities regarding ICT Acceptable Use, including storage of ICT, unacceptable use, internet use, email, passwords, remote working and reporting security incidents
- To inform staff, pupils and parents about safe mobile technology use in school.
- To ensure staff, pupils and parents are familiar with the school policy on pupil use of personal mobile technology in school.
- To highlight the child protection issues of using camera and video phone technology in the school such as Youth Produced Sexual Imagery or "Sexting", and the consequences of this.
- To determine exactly when and where mobile phone use is permitted in the school.
- Offer safety guidelines to the pupils / staff on general mobile phone use.
- To outline the consequences of not adhering to the school Mobile Technology policy.
- To outline who has responsibility in the case of loss, theft or damage of mobile technology.

This policy applies to

- Any individual using or accessing school ICT;
- School owned or leased ICT such as PC's; laptops; notebooks; smart phones; software; services, storage media and network resources.

2. General Responsibilities

- You must protect your user name, password, and security token (if used) against misuse.
- All ICT must be subject to access control to ensure only authorised persons can access the ICT.
- You must operate a clear screen policy when you leave your device unattended e.g. locking your computer by pressing the Windows key and the 'L' key simultaneously or by engaging the lock screen on your smartphone.
- You must protect portable devices and removable media at all times. When not in use during school hours they must be subject to appropriate security e.g a locked screen. When not in use outside of school hours or away from school, they must be under lock and key.
- You must ensure all portable ICT used to store or process sensitive information, such as personal data, is encrypted.
- You must ensure all ICT is returned to F1 Group when no longer required. This is to ensure devices are securely wiped or destroyed.
- You must only access or attempt to access ICT that you have been authorised to access.

- You must only access or attempt to access information for official school purposes aligned with your role and this must be on a need to know basis.
- You must Report any loss, theft, damage or compromise of a school device promptly to the Headteacher and data protection officer

3. Unacceptable Use

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

Staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies.

4.Email

- You must only send school emails from your own authorised account.
- You must check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Particular care must be taken when using auto complete in your email client as an unintended email address may be used in error.
- You must not use personally owned email accounts to conduct school business or to transmit or receive school information.
- You must take care when opening an attachment or clicking on any link within any email unless you are confident the email is legitimate.
- Suspicious email should be deleted and must not be forwarded to other recipients.
- If you suspect an email contains malware please contact F1 Group, 01522 508080.
- When sending an email to more than one recipient and it is necessary to protect email addresses the blind carbon copy (BCC) feature must be used.
- When sending sensitive information via email you must ensure it is done so securely.
- Personal use of school email shall be reasonable, proportionate and occasional and must not interfere with the performance of your role or the performance of the system.
- Delegate access to email accounts must only be provided following a clear business need and only when authority is provided by the email account owner, or in their absence, the Head Teacher. To arrange delegate access please contact Heather Brunsden, Data Protection Officer.
- Delegate access must not be provided by supplying details of a User's credentials i.e. username and password.
- When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must not open it or stop immediately if the email has been opened.

Email messages are required to be disclosed in legal proceedings or in response to subject access requests from individuals under the UK GDPR and the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

5. Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the Headteacher.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

6. Passwords

- Passwords must not be shared and must be protected from unauthorised disclosure.
- When creating a passwords ensure it is not easily guessable e.g. 'letmein123',
- 'Password1' and avoid using keyboard patterns or sequential numbers e.g. qwerty, 12345.
- Passwords must be minimum 8 characters in length and include a mixture of upper/lowercase, numbers and special characters.
- Passwords must not be recorded unless it is done so securely and you are the only one who can access is it.
- The same password must not be used across different accounts (work and private) and/or applications.
- Default passwords must be changed.
- If school email is accessed on a non-work device, the email address should be protected by a secure password or identification.

7. Removable Media

- Removable media which contains sensitive information such as personal data must be encrypted. Removable media includes USB flash drives, CDR, DVDR, removable hard drives.
- Removable media from an unknown source must not be introduced to school ICT as it may contain malware designed to harm school systems.

8. Remote/Mobile Working

- Additional care must be taken when working outside of school premises and you must ensure that reasonable safeguards are taken to manage the increased likelihood of a security incident.
- You must only remove ICT from school premises when there is a clear business need.
- You must prevent inadvertent disclosure of information and avoid being overlooked when working.

- When removing ICT from school premises, and it contains sensitive information such as personal data, only do so if it is encrypted.
- You must avoid storing ICT in an unoccupied vehicle unless more secure options are unavailable. If it is unavoidable then you must place the ICT out of sight, in the locked boot of the vehicle.
- ICT must never be stored in a vehicle overnight.
- Portable devices must connect to the school's ICT network on at least a monthly basis in order to receive security updates. You must ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.

9. Staff use of mobile phones (this includes school staff, volunteers and trustees)

- The school allows staff to bring in personal mobile phones and devices for their own use. Staff are advised to use passwords/pin-codes to ensure their phone cannot be used by an unauthorised person and must store them away safely during working hours. Personal mobile phones should not be out on desks during working hours.
- There should be no personal use of mobile devices during pupil contact time or working hours. In exceptional circumstances (for example, a family emergency), staff should seek permission from SLT to use their personal mobile device when in contact with pupils.
- Staff should not give their personal mobile phone numbers or personal email addresses to pupils, parents or carers.
- Staff personal mobile phones should not be used for any school related matters except in exceptional circumstances, unless authorised to do so by a member of SLT .
- If staff access their school email on a non-work device, the email address should be protected by a secure password or form of identification
- Only the mobile devices belonging to school may be used to take appropriate and relevant images of pupils; for example, for observations/school events, unless authorised to do so by a member of SLT in an exceptional circumstance. In these cases, the photos must be deleted immediately after the event and verification of the deletion should be checked.
- Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- During off-site visits, staff will be provided, where possible, with a school mobile phone and this should be used to contact school or parents should an emergency arise. However, if a school mobile device is not available then staff can use their personal mobile device with authorisation from a member of SLT.
- There may be times where staff are required to contact families from their own mobile device. If this is required, staff will ensure that they withhold their number, thus protecting the security and privacy of staff's details.

10.Pupil use of mobile phones

We do not allow pupils to bring mobile phones into school and if you do, be aware that they will be taken by your class teacher, passed to the office and your parent/carer must collect these.

11. Visitor use of mobile phones

- Visitors should not use their personal mobile devices during pupil contact. These should be kept in a lockable key safe.
- Parents and carers are reminded that if you are permitted to take photos during a school performance or event, to not share them on social media or for any other purpose.
- School Photographers will be treated as any other visitor and appropriate levels of supervision will be in place at all times.
- In exceptional circumstances, visitors may keep their mobile phones with them, but must sign a mobile phone agreement.

12. Responsibility for mobile phones and other mobile devices

The school accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile technology. It is the responsibility of staff, parents and visitors to make sure that mobile technology is properly insured.

13.Youth Produced Sexual Imagery or 'Sexting'

Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18. All incidents involving youth produced sexual imagery will be responded to in line with our Safeguarding and Child Protection policies.

14.Reporting Security Incidents

All security incidents and suspected security incidents must be reported in accordance with the school's Security Incident Policy.

If you identify suspicious activity while using ICT or believe that you are the victim of malware e.g. a virus, you must stop what you are doing, power off your ICT and report it immediately.

You must report all security incidents to Heather Brunsden, Data Protection Officer.

15. Monitoring

The school reserves the right to monitor its communication systems and services.

This includes, but is not limited to, email, telephone conversations, electronic messaging, internet use, and system access.

Monitoring is used by the school for the following purposes:

To maintain and ensure security of systems and information;

To check for unauthorised use;

To establish facts relevant to school business;
To ensure quality assurance and ensure that procedures are being followed;
To undertake disciplinary, performance, and capability proceedings; and
To prevent or detect crime.

16. Further Information

For further information regarding ICT acceptable use within the school please contact:
Heather Brunsden
Senior Administrator/Bursar
heather.brunsden@manorleasinfant.org
01522 681810

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

17.Policy Review

This policy will be reviewed on an annual basis by the Headteacher and a trustee. The approved policy will be shared with the trustee board.