MANOR
MULTI ACADEMY TRUST

ICT & Electronic Devices Policy

Date adopted by the MAT	July 2024
This policy is scheduled for review on	Annually

Contents

Statement of intent

Manor Multi Academy believes that ICT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personal electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- MAT & School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy and Online Safety Policy.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Data Protection Policy
- Cyber-security Policy
- Records Management Policy

Roles and responsibilities

The Directors have the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The CEO / headteacher is responsible for:

- Reviewing and amending this policy with the ICT Admin and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is carried out daily by the MAT ICT Admin.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices if required or incident occurs for the purpose of ensuring the effectiveness of this policy and security of the MAT.
- The ICT Admin is responsible for:
- Carrying out regular checks on internet activity of all user accounts and to report any inappropriate use to the headteacher.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher.
- Remotely viewing or interacting with any of the computers on the network. This may be done randomly to implement this policy and to assist with any support issues.
- Ensuring routine security checks are carried out on all school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and devices.
- Disabling user accounts of staff who do not follow this policy, at the request of the CEO / headteacher.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of personal devices to the DPO.

The DPO is responsible for:

- Ensuring that all school-owned devices have security software installed, to protect sensitive data in cases of loss or theft.

- Inform users that personal devices used with school accounts must be secured with a pin or password and have up to date operating system and firmware with protective software to prevent virus or malware.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that devices connected to the MAT system & network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the MAT Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the headteacher or ICT Admin, subject to their approval, before using school-owned devices for personal reasons.
- Requesting permission to loan school equipment and devices from the headteacher or ICT Admin.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours and ensuring these devices are submitted for security checks on a regular basis.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the DPO and Head of ICT.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing an Acceptable Use Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

ICT Admin is responsible for the maintenance and day-to-day management of the equipment, as well as the device loans process.

The School Business Manager is responsible for:

- Help maintain an Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance procedures.
- Overseeing order and purchase requests for electronic devices.

Classifications

School-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- iPad
- Monitors
- Keyboards
- Mouse

- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

Acceptable use

This policy applies to any device connected to the school's network and computers. The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy and the Acceptable Use Agreement.
Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.
Any member of staff found to have breached the school's Data Protection Policy or relevant legislation could face disciplinary action based on the seriousness of offence.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.
Since ICT facilities are also used by pupils, the school will strongly consider acceptable use agreements in place for pupils – staff will ensure that pupils comply with these. Pupils found to have been misusing the ICT facilities will be reported to the headteacher.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.
Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download illegal file types or software.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Report any spam or possible compromise to the Head of ICT immediately without delay

All data will be stored appropriately in accordance with the school's Data Protection Policy and no personal information of anyone but themselves must reside on their own personal device(s). Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.
School-owned electronic devices will not be used to access personal social media accounts.
Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.
Copyrighted material will not be downloaded or distributed.
School-owned devices will be taken home for work purposes only, once approval has been sought from the headteacher and ICT Admin.

School equipment that is used outside the premises, e.g. laptops / iPads, will be returned to the school when the employee leaves employment, or if requested to do so by the CEO / headteacher or Head of ICT.
While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.
Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

MAT / School owned mobile phones must only be used for official business and not personal. The device must be kept physically secure and have a secure pin and managed by the MAT device management software.

Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.

More details about acceptable use can be found in the staff Technology Acceptable Use Agreement.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

Emails and the internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proof-read by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The school will be liable for any defamatory information circulated either within the school or to external contacts.

The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications.

School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails being sent to external recipients will contain the MAT / school standard confidentiality notice. That notice will normally be configured as a signature by the ICT Admin and will not be removed.

Personal email accounts will only be accessed via school computers outside of work hours and must be used incognito and access approved by the ICT Admin. Staff will ensure that access to personal emails never interferes with work duties.

Staff linking work email accounts to personal devices, subject to the headteacher's approval, will need to submit their devices for routine security checks on a termly basis.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.
Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.
Purchases for school equipment will only be permitted to be made online with the permission of the headteacher, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the School Business Manager. This is in addition to any purchasing arrangement followed according to the MAT / school's Finance procedures.
Any suspicious emails will be recorded in the incident log and will be reported to the headteacher. All incidents will be responded to in accordance with the Online Safety Policy.

Staff will be subject to simulation periodic email testing of phishing and other forms of possible compromise. If the user repeatedly fails this test then further training will be required and if it continues could be considered as negligence and further action could be sought.

Portable equipment

All data on school-owned equipment will be synchronised with MAT cloud solutions regularly and backed up every day.
Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked in location when they are not in use.
Portable equipment will be transported in its protective case, if supplied.
Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

Personal devices

Staff members will use personal devices in line with the MAT / school's Acceptable Use, Data Protection and Cyber Security Policies.
All personal devices that are used to access the school's online portal, systems, or email accounts, e.g. laptops or mobile phones, will be declared and approved by the headteacher before use and submitted for the routine checks outlined in Safety and security section of this policy.
Staff using their own devices will the device is up to date, has anti-virus installed and secured with a pin or password and that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by the ICT Admin. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.
Approved devices will be secured with a password or 2 factor access control, e.g. Authenticator app.

Members of staff will not contact pupils using their personal devices.
Inappropriate messages / emails will not be sent to any member of the school community.
Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.
Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.
During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in location.

Removable media

Removable media is not allowed.
MAT systems do not allow copying information to removable media.
The ICT Admin will encrypt all removable media with appropriate security measures if it is an exceptional circumstance that it is required. This method will be avoided.
Removable media found will be disposed of securely by the ICT Admin and reported to the Head / CEO.

Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data containing any personal information or organisational business files are kept confidential and no data is copied, removed or adapted.

Storing messages

Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and are encouraged to delete emails when no longer required.
Information and data on the MAT / school's infrastructure and devices will be kept in an organised manner and should be placed in a location of an appropriate security level.
If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT Admin.
Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the headteacher, as appropriate.

Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT Admin or headteacher. Certain items are asset registered and security marked; their location is recorded by the School Business Manager for accountability. Once items are moved after authorisation, staff will be responsible for notifying the School Business Manager of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed every six months. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
  - Any material that is illegal
  - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
  - Online gambling
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
  - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the ICT Admin or the headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Attempted hacking of MAT / School systems or any external entities
- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the ICT Admin or headteacher. This is in addition to any purchasing arrangements followed according to the Finance procedures.
- Use or attempt to use the school's phone lines for any use other than school or MAT business related activity.

- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance procedures.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including dismissal.
- Use the ICT facilities for personal use without the authorisation of the headteacher. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Use other staff codes for access including printing / copying facilities.
- Be wasteful of resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image inappropriately such as beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's underwear, genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy.
If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the CEO / headteacher as an urgent safeguarding concern. Failure to report an incident will also be taken seriously knowing the risk to the MAT / School and ultimately the children and other staff.

Purchasing

Funding for electronic devices, predetermined by the MAT CFO, will be available each year on request from the School Business Manager.

Requests made for equipment or electronic devices that exceed the predetermined amount allocated will require discussion and authorisation by the CEO or Directors.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf unless permission has been sought from the headteacher.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the headteacher.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The School Business Manager will seek advice from the ICT Admin and professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The MAT ICT Admin will maintain a Fixed Asset Register which will be used to record and monitor the MAT / school's assets. All equipment and electronic devices purchased using school funds will be added to this register.

Any old devices will then be disposed of following the WEEE directive arrange by MAT ICT Admin.

Safety and security

The school's network and ICT facilities will be secured at all times.

Filtering of websites is managed MAT centrally by ICT Admin and will ensure that access to websites with known malware are blocked immediately. Staff MUST contact ICT Admin and report if any websites need to be blocked.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated on a termly basis.

The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on an annual / contract renewal basis.

Members of staff will ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, on a daily basis. Devices will prompt to restart and the user must allow this to complete. It will automatically do this after 30 days if postponed.

Approved personal devices will also be submitted on a termly basis, to the MAT ICT Admin, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the school reserves the right to decline a request to use a personal device.

Records will be kept detailing the date and time, owner of a device and device type, on which the routine checks have taken place.

Programmes and software will not be installed on school-owned electronic devices without permission from the MAT ICT Admin.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the MAT ICT Admin.
Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the MAT ICT Admin, may be subject to disciplinary measures.
All devices will be secured by a password and / or 2 Factor authentication.
Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.
Devices will be configured so that they are automatically locked after being left idle for a set time. Staff are encouraged NOT to leave their laptop unattended and logged on. Staff need to lock their device when leaving and physically secure if needed.
All devices must be encrypted using a method approved by the DPO.
Further security arrangements are outlined in the Data Protection and Cyber-security Policies.

Loss, theft and damage

For the purpose of this policy, “damage” is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT Admin
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation
- Hacking

The school’s insurance will cover school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises.
Staff members will use school-owned electronic devices within the parameters of the school’s insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.
Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.
The ICT Admin, CEO and headteacher will decide whether a device has been damaged due to the actions described above.
The ICT Admin will be contacted if a school-owned electronic device has a technical fault.

The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

Implementation

Staff will report any breach of this policy to the headteacher.
Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.
Use of the telephone system will be logged and monitored.
Use of the school internet connection will be recorded and monitored.
The School Business Manager will conduct random checks of asset registered and security marked items.
The MAT ICT Admin will check computer logs on the school network on a termly basis.
Unsuccessful and successful log-ons will be logged on every computer connected to the school's network.
Unsuccessful and successful software installations, security changes and items sent to the printer will also be logged.
The MAT ICT Admin may remotely view or interact with any of the devices on the school's network. This may be used randomly to implement this policy and to assist in any difficulties.
The school's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.
The school's database systems are computerised. Unless given permission by the MAT ICT Admin, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.
All users of the database system will be issued with a unique individual password. Staff will not, under any circumstances, disclose this password to any other person.
Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.
User accounts will be accessible by the headteacher and the ICT Admin if required.
Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.
Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.
A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

Monitoring and review

This policy will be reviewed annually by the ICT Admin and the headteacher.
Any changes or amendments to this policy will be communicated to all staff members by the headteacher.