Staff, Governor and Trustee Acceptable Use Policy (ICT and Electronic Devices)

Version	2.0
Date Policy Last Reviewed	September 2023
Policy Type	Mandatory
Owner	CEO
Approved By	Trust Board
Approval Date	10th October 2023
Review Date	September 2024

Review Date & Summary Changes

Review Date	Summary Changes
September 2023	5.2 The trust email account should be used for all trust/school business. Personal accounts should not be used for school/trust business-related communications.

Approved by	Date
Chief Executive Officer	10/10/23
Chair of Trustees	10/10/23

Contents:

Statement of intent

Omega Multi Academy Trust the Trust), and each of its constituent schools, believe that ICT plays an important part in both teaching and learning over a range of subjects, and accepts that both school-owned and personal electronic devices are widely used by members of staff. The Trust 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 Trust 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.
- Trust/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.

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

1. Legal framework

1.1 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)

1.2 This policy operates in conjunction with the following Trust/school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images Policy
- Trust Financial Regulations

2. Roles and responsibilities

2.1 The Board of Trustees has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

2.2 Trust IT Managers:

- Reviewing and amending this policy with the Chief Executive Officer, Chief Finance and Operations Officer and Data Protection Officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- Ensuring that all school-owned electronic devices have security software installed, to protect sensitive data in cases of loss or theft.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

2.3 Headteachers and Trust Executive Leaders are responsible for:

- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources.
- 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 for the purpose of ensuring the effectiveness of this policy.

2.4 ICT Network Managers/Technicians are responsible for:

- Carrying out checks on internet activity of all user accounts and to report any inappropriate use to the Headteacher/Chief Executive Officer, as appropriate.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the Headteacher/Chief Executive Officer, as appropriate.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.
- Ensuring routine security checks are carried out on all school-owned devices to check that appropriate security measures and software have been updated and installed.
- 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 Trust/school's data, information, network and computers.
- Disabling user accounts of staff who do not follow this policy, at the request of the Headteacher/Chief Executive Officer, as appropriate.
- Assisting the Headteacher/Chief Executive Officer as appropriate, 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 Data Protection Officer.

2.4 Staff members are responsible for:

- Requesting permission from the headteacher or ICT technician, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the headteacher or Chief Finance and Operations Officer.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours and ensuring these devices are secure, in keeping with the requirements of school/trust-owned devices.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the Trust (as outlined above).
- Reporting misuse of ICT facilities or devices, by staff, to the Headteacher or Chief Executive Officer, as appropriate.
- Reading and signing the Trust IT Acceptable Use Agreement, to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

2.5 The School Business Manager (or equivalent), in collaboration with trust IT Managers, are responsible for:

- Maintaining a Fixed Asset Register to record and monitor the Trust/school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Financial Regulations.
- Overseeing purchase requests for electronic devices.

3. Classifications

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

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Camcorders
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Pagers
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

4.1 This policy applies to any computer or other device connected to the school's network and computers.

4.2 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

4.3 Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

4.4 Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

4.5 Any member of staff found to have breached the school's Data Protection Policy or relevant legislation could be subject to disciplinary processes.

4.6 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.

4.7 Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

4.8 Pupils found to have been misusing the ICT facilities will be reported to the Headteacher, or senior leader with designated responsibility for the management of behaviour.

4.9 School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

4.10 Any illegal, inappropriate or harmful activity will be immediately reported to the Headteacher, or Chief Executive Officer, as appropriate.

4.11 Members of staff should 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 large capacity files 500MB without permission from the ICT technician.
- 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.

4.12 All data will be stored appropriately in accordance with the school's Data Protection Policy.

4.13 Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

4.14 School-owned electronic devices will not be used to access personal social media accounts.

4.15 Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

4.16 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.

4.17 Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

4.18 Copyrighted material will not be downloaded or distributed.

4.19 School-owned devices will be taken home for work purposes only, once approval has been sought from the headteacher and ICT technician. Remote access to the school network will be given to staff using these devices at home.

4.20 School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the Headteacher, or Chief Executive Officer.

4.21 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/Chief Executive Officer or in the case of a personal emergency.

4.22 Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

4.23 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.

4.24 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.

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

4.26 More details about acceptable use can be found in the staff Technology Acceptable Use Agreement ADD AS AN APPENDIX??

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

5. Emails and the internet

5.1 The Trust's email system and internet connection are available for communication and use on matters directly concerned with school/Trust business.

5.2 The trust email account should be used for all trust/school business. Personal accounts should not be used for school/trust business-related communications.

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

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

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

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

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

5.8 The Trust/school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. Trust/school email addresses should not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

5.9 All emails that are sent or received will be retained within the school for a period of **12 months** dependent on the information contained. The timeframe will be altered where an inbox becomes full.

5.10 All emails being sent to external recipients will contain the school standard confidentiality notice. That notice will normally be configured as a signature by the IT Managers and will not be removed.

5.11 Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the IT Managers. Staff will ensure that access to personal emails never interferes with work duties.

5.12 Staff linking work email accounts to personal devices, subject to the headteacher's/Chief Executive Officer's approval, will sign the IT Acceptable Use Agreement.

5.13 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.

5.14 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 Trust, and the recipient. Staff will never commit the school/Trust to any obligations by email or the internet without ensuring that they have the authority to do so.

5.15 Purchases for school equipment will only be permitted to be made online with the permission of the Headteacher or appropriate budget holder (subject to supplier approval processes as detailed within the trust's financial regulations). A receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase order will be made for the purchaser and the School Business Manager (or equivalent). This is in addition to any purchasing arrangement followed according to the school's Financial Regulations.

5.16 Any suspicious emails will be reported to the Trust IT Manager. All incidents will be responded to in accordance with the Online Safety Policy.

6. Portable equipment

6.1 Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely when they are not in use.

6.2 Where the Trust/school provides mobile technologies, such as phones/laptops, for off-site visits and trips, staff will only use these devices for school/trust-related activity.

7. Personal devices

7.1 Staff members will use personal devices whilst on the Trust/school premises, in line with this Policy.

7.2 All personal devices that are used to access the Trust/school's online portal, systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the headteacher before use.

7.3 By using their own devices to access school/Trust systems, they are agreeing that they understand their responsibilities under this policy and devices should be secured with a password or biometric access control, e.g. fingerprint scanner.

7.4 Members of staff will not contact pupils or parents using their personal devices.

7.5 Personal devices will only be used for off-site educational purposes when mutually agreed with the headteacher/Chief Executive Officer.

7.6 Inappropriate messages will not be sent to any member of the school community.

7.7 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.

7.8 Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

7.9 During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in a secure location.

8. Removable media

8.1 No school/trust data should be stored on removable media without the express consent of the IT Manager.

9. Cloud-based storage

9.1 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 is kept confidential and no data is copied, removed or adapted.

10. Storing messages

10.1 Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of after no more than six months.

10.2 Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

10.3 If a member of staff is unsure about the correct message storage procedure, help will be sought from the IT Manager/Network Manager as appropriate.

10.4 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. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

11.1 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 IT Technician, Network or IT Managers or the Headteacher. Certain items are asset registered and security marked; their location is recorded for accountability. Once items are moved after authorisation, staff will be responsible for notifying the Network 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 180 Days. 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 IT Manager/Network Manager or the Headteacher/Chief Executive Officer.
- 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.
- Use or attempt to use the 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 Manager/Network Manager or Headteacher. This is in addition to any purchasing arrangements followed according to the Trust's Financial Regulations.
- Use or attempt to use the Trust/school's phone lines for internet or email access unless given authorisation by the headteacher. This will include using or attempting

to use any other form of hardware capable of telecommunication, regardless of ownership.

- Use any chat-lines, bulletin boards or pay-to-view sites on the School/Trust internet connection. 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 Financial Regulations.
- Knowingly distribute or introduce a virus or harmful code onto the Trust/school's network or computers. Doing so may result in disciplinary action.
- Use the ICT facilities for personal use without the authorisation of the headteacher/Chief Executive Officer. 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 Trust/school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT 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 beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

11.2 Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

11.3 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 headteacher.

12. Safety and security

12.1 The Trust/school's network will be secured using firewalls in line with the Data Policy

12.2 Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the IT Managers.

12.3 Approved anti-virus software and malware protection will be used on all approved devices and will be updated frequently (daily if updates are available).

12.4 The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on a daily basis, as and when updates are available.

12.5 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, as required.

12.6 Programmes and software will not be installed on school-owned electronic devices without permission from the ICT Network Manager/Trust IT Managers.

12.7 Staff will not be permitted to remove any software from a school-owned electronic device without permission from the ICT Network Manager/Trust IT Managers

12.8 Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the ICT Network Manager/Trust IT Managers, may be subject to disciplinary measures.

12.9 All devices will be secured by a password or biometric access control.

12.10 Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

12.11 Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 15 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.

12.12 All devices must be encrypted using a method approved by the Trust IT Managers/Data Protection Officer.

13. Loss, theft and damage

13.1 For the purpose of this policy, **"damage"** is defined as any fault in a trust/school-owned electronic device caused by the following:

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

13.2 The Trust/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.

13.3 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.

13.4 Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

13.5 If a trust/school-owned device is lost or stolen, or is suspected of having been lost or stolen, the Data Protection Officer and the IT Managers will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the trust, school, its staff and its pupils, and that the loss is reported to the relevant agencies.

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

14. Monitoring and review

14.1 This policy will be reviewed annually by the IT Managers, in consultation with the Chief Executive Officer, Chief Finance and Operations Officer and the Data Protection Officer.

14.2 Any changes or amendments to this policy will be communicated to all staff members by the headteacher.

14.3 The scheduled review date for this policy will be 1 September 2024