Manor MAT Digital & Data Acceptable Use Agreement Policy 2024-25

Date approved	8.10.24
Approved by	Directors
Date adopted by the MAT	1.9.24
This policy is scheduled for review on	Annual or on updates

Contents

Policy Statement

This policy outlines Manor Multi Academy Trust's ('we' / ''our' / 'us') expectations of our employees' ('you') in relation to acceptable use of Information Communications Technology (ICT) equipment, facilities and data within our Trust. ICT is seen as beneficial to all our staff members in supporting learning, teaching, research, administration and approved business activities of our Trust. Our ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users in our Trust. This could also lead to a breach of the data protection rights of individuals, resulting in harm to you and us.

We are committed to equality and value diversity. As such we are committed to fulfilling our Public Sector Equality Duty (Equality Duty) obligations and expect all staff and volunteers to share this commitment.

This policy should also be applied in accordance with our Staff Code of Conduct, Dignity at Work, Safeguarding and Child Protection, Safer Recruitment, and our suite of ICT policies and procedures including our Social Media Policy. Copies of all policies and procedures can be accessed via the **All MAT Staff** area on Teams.

The Equality Duty requires us to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, and victimisation.
- Advance equality of opportunity.
- Foster good relations between people who share protected characteristics, such as age, gender, race and faith, and people who do not share them.

If you consider that any of our practices, policies or procedures may be indirectly discriminatory, you should report your concerns and the basis for them to your line manager, who will take appropriate action and ensure that you receive a written response in respect of the concerns that you have raised.

This policy does not form part of your contract of employment. We reserve the right to amend or withdraw this policy at any time.

We are responsible for ensuring the effective implementation of this policy. As part of equality monitoring we will review and monitor the operation and impact of the policy on a regular basis and in accordance with the policy review date. As part of this monitoring and review this policy will be equality impact assessed.

Scope

This policy applies to or Directors, Parent and Community Advisory Forum (PCAF) representatives, employees, workers, agency workers, consultants, casual workers, contractors, volunteers and pupils whether during working hours or otherwise. You must ensure you have read this Policy before commencing use of our information and

communication technology. Failure to do so will not be accepted as a mitigation factor should a problem arise during employment or period of study.

This Policy provides information which underpins our Staff Code of Conduct, and Disciplinary Policy and Procedures. Copies of these policies and procedures can be accessed via the **All MAT Staff** area on Teams.

Aims & Principles

The aim of this policy is not to impose restrictions that are contrary to the established culture of openness, trust and integrity within our Trust. This policy is designed to protect all authorised users from illegal or damaging actions by individuals, either knowingly or unknowingly.

Identified update changes for this version:

a) Artificial Intelligence statements: 3.14 -15
b) Artificial Intelligence unacceptable use: 4.1.18 – 23
c) Wearable Technology

Definitions

For the purpose of this policy the following definitions are applied:

- "**ICT Device**" means any laptops, tablets, telephones, smartphones, desktop computer, console, printer, speaker, camera or other electronic equipment that could be used for the carrying out of our business or the processing or storing of information. Please also refer to our ICT and Electronic Devices Policy available in the **All MAT Staff** area on Teams.

- "ICT Facilities" means all devices, facilities, systems and services including, but not limited to, network infrastructure, ICT Devices, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of our ICT service.

- "**Users**" means Directors, PCAF representatives, staff, pupils, trainees, volunteers, temporary guests, and all other persons authorised by us to use our ICT Facilities.

- "**Personal use**" means any use or activity not directly related to the user's employment, study or purpose.

- "**Authorised Personnel**" means employee(s) authorised by us to perform systems administration and/or monitoring of our ICT Facilities.

- "**Materials**" means files and data created using our ICT Facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

- **AI** is an abbreviation of Artificial Intelligence.

Acceptable Use Policy

Our ICT Facilities should only be used to support your employment role including learning, teaching, research, administration and approved business activities of our Trust. Our ICT Facilities must not be used for personal commercial, political, charitable, and other such activities unless expressly authorised by us.

Device security and safe practices

We employ various measures to protect the security of our computing resources and user accounts. Users should be aware that we cannot guarantee such security. Users should therefore engage in safe computing practices by always adhering to our ICT Policies, backing up files, and promptly reporting any misuse or violations of this policy.

All devices that use our ICT Facilities, and that are capable of supporting software updates, security updates and automatically updating anti-virus products, must be configured to perform such updates. Or devices are periodically checked if unable to centrally manage where possible to ensure compliance.

Users' accounts and passwords must not be shared with anyone. You are responsible for the security of your passwords, accounts and for setting account and file permissions. Disclosure of account or password information may result in disciplinary action.

Email use and Instant Messaging

Please refer to our ICT and Electronic Devices Policy, available in the **All MAT Staff** area on Teams.

Authorised Access

Should an individual user account support permitting other users to access the account, such as delegating access to an email system's inbox or calendar, only the account owner – or highest level senior authority in the Trust/Academy - is authorised to permit access to be granted. The account owner must not permit access to any ICT facility or user account to external or third-parties, without explicit written permission from the Data Protection Officer (DPO) or Head of ICT.

Occasionally we may need to access information held by a User within ICT facilities, including, but not limited to, email, files stored on a personal computer or file storage or on other file store (e.g. OneDrive or Teams) or backup media. This will usually occur when a User is absent, either ill or on leave, and a situation arises which requires a rapid response. Users must be made aware that we reserve the right to obtain access to files stored upon systems and services owned by us, and that the privacy of personal material stored upon such systems and services in the event of authorised access cannot be guaranteed.

In the event that access is required to another user's individual account(s), and the account's owner cannot provide such authorisation, the Account Access Request must be authorised by the CEO or CEA. It is intended that these arrangements are for exceptional circumstances only and access requests will only be considered if they demonstrate that delay will cause disproportionate damage to the Trust.

In exceptional circumstances, Authorised Personnel may need to make changes to user data or storage for the purposes of operating and providing a system or service. Where reasonable, Authorised Personnel should request permission of the data owner unless the situation is of such urgency as to make this impracticable. However, after such a change the file owner should be informed of the change and the purpose as soon as possible. The Authorised Personnel may not, without specific authorisation from the DPO or Head of ICT, modify the contents of any file in such a way as to damage or destroy information.

Copyright

You must abide by all applicable laws and Trust policies to protect the copyrights and intellectual property rights of others. Copyrighted works may include texts, cartoons, articles, photographs, songs, videos, software, graphics, and other materials. This includes the use of the internet, as many of the materials available through the internet are protected by copyright. It is your responsibility to assume that materials found upon the internet are copyrighted unless the materials contain an express disclaimer to the contrary. You must obtain permission of the creator or publisher to copy or use software or other copyrighted materials written or created by others and must abide by contracts and agreements controlling installation and use of such software and other materials.

Ethical and legal implications

Usage of the ICT Facilities must be in an ethical and legal manner and in accordance with our Dignity at Work Policy and Procedure and suite of ICT policies as available in the **All MAT Staff** area on Teams (including ICT and Electronic Devices and Social Media. Usage of the system to harass, defame, or invade the privacy of others, or to send or receive obscene materials, is not allowed and may result in disciplinary action under policies controlled by us or prosecution under applicable laws.

You must not use the ICT Facilities to hold or process personal data except in accordance with the Data Protection Legislation and our Data Protection Policy, available both in the **All MAT Staff** area on Teams and on our website.

Personal/Other Use

Should you wish to use our ICT Facilities for personal, personal commercial, political, or charitable or other activity not directly related to your position within the Trust, permission must be expressly granted by us via a senior member of the team. Any such use must not hinder or interfere with your duties and must not prevent the legitimate use of these facilities by others. You may not use our ICT Facilities to store personal non-work-related information or materials on the ICT Facilities (e.g. eBooks, music, home videos, photography), and use of the ICT Facilities is provided with no expectation of privacy.

If permission is granted for use which is personal, personal commercial, political, or charitable or other activity not directly related to your position, the ICT Facilities are used entirely at your own risk. We will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of ICT Facilities. Although we take reasonable care to prevent the corruption of information, we do not give any warranty or undertaking to you about the integrity of information and accept no responsibility for the malfunctioning of any computing hardware, software or facility and/or any loss of any data or software or the failure of any security or privacy mechanism. No claim shall be made against us, our employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act of neglect of us, our employees or affiliates.

Professional conduct is observed during the working day and beyond with the aid of device monitoring, filtering and logging wherever the device is located. You must be aware that personal activities using work equipment with examples such as online shopping, gaming, watching media content and any other non-listed personal activities could result in action taken if not approved by line manager and does not contravene your normal working conditions or professional conduct.

Artificial Intelligence (AI)

The use of AI tools must be used with integrity, honesty, and in a manner that respects the rights, privacy, and dignity of individuals. You must safeguard and protect sensitive company data, intellectual property, and confidential information when using AI tools.

Treat every bit of information you provide to an AI tool as if it will go viral on the Internet, attributed to you or the Trust, regardless of the settings you have selected within the tool (or the assurances made by its creators). AI tools may be useful but are not a substitute for human judgment and creativity.

Wearable personal technology IS permitted but only for basic use only within working hours. If you engage in using this technology whilst working, then this may result in further action

being taken and you may be asked to remove the device. Messaging, social media use, photographs, video or recordings must not take place using this technology whilst at work. Further information can be found in our ICT and Electronic Devices policy, available in the **All MAT Staff** area on Teams.

Cyber security

Please refer to our Cyber Security Policy, available in the **All MAT Staff** area on Teams.

Unacceptable Use

We reserve the right to block, disconnect or otherwise prevent what we consider to be unacceptable use of our ICT Facilities. Unacceptable use includes, but is not limited to:

a) All actions or activities that are illegal or in conflict with our policies, procedures, processes and regulations or which breach contracts or policies applied to us by a third party through a valid service contract or agreement.

b) Using our ICT Facilities for access, creation, modification, storage, download, hosting or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material.

c) Publishing materials or making statements which we may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience.

d) Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any copyrighted sources and installation of any copyrighted software for which we do not have an active licence or explicit permission of the copyright owner, is strictly prohibited.

e) Authoring or sending any form of electronic communications or messages, including, but not limited to, videos, chats, messages and/or emails that were unsolicited and may be considered inappropriate, junk, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person.

f) Unauthorised recording, “screenshotting”, capturing, photographing or any other means of observing and/or documenting the materials of an ICT device, without prior notification and agreement.

g) Unauthorised transmission, distribution, discussion or disclosure of information gained through your presence within our Trust or through the use of our ICT Facilities.

h) Connecting any non-approved ICT device, system or service (including wireless access points) to our networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel.

i) Unauthorised access (or attempted unauthorised access) to any ICT Facilities provided by us.

j) Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the ICT Facilities.

k) Causing any damage to ICT Facilities, including through the consumption of food or drink, or moving or removing such facilities without authorisation. We reserve the right to charge for any damage caused.

l) Attempting to modify, alter or in any way interfere with ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites without the written authorisation or delegated permission from Authorised Personnel.

m) Introduction of unauthorised and/or malicious software or programs into our ICT Facilities, including, but not limited to: unlicensed software, viruses, worms, Trojan horses or logic bombs; by downloading, creating or using any program, tool or item of software designed to monitor damage, disrupt or interfere with the functioning of ICT Facilities, user accounts or data.

n) Effecting security breaches or disruptions of network communication, including, but not limited to: accessing or modifying data (or data headers) of which you are not an intended recipient or logging into an ICT system or service, or account, that you are not expressly authorised to access. Disruption includes, but is not limited to: network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

o) Executing any form of network monitoring including any data capture, port scanning or security scanning without written authorisation or delegated permission from Authorised Personnel.

p) Registering for any system or service, including, but not limited to: social media accounts, web applications, domain names, which includes the name of our Academy or any similar name, or abbreviation that may mislead the public into believing that the domain name refers to our Trust.

q) Acting in any way that directly or indirectly causes disruption to others' use of our ICT Facilities or using ICT Facilities to disrupt or deny the use of ICT Facilities of third parties at any time.

r) Using AI tools to make or help you make employment decisions about applicants or employees, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations.

s) Uploading or inputting any confidential, proprietary, or sensitive Trust information into any AI tool. Examples include passwords and other credentials, protected health information, personnel material, information from documents marked Confidential, Sensitive, or Proprietary, or any other non-public Trust information that might be harmful to the Trust if disclosed. This may breach your or our obligations to keep certain information confidential and secure, risks widespread disclosure, and may cause our rights to that information to be challenged.

t) Uploading or inputting any personal information (names, addresses, likenesses, etc.) about any person into any AI tool.

u) Representing work generated by an AI tool as being your own original work.

v) Integrating any AI tool with internal Trust software without first receiving specific written permission from your supervisor and the IT Department.

w) Using AI tools other than those on the approved list from the ICT Department. Malicious chatbots can be designed to steal or convince you to divulge information.

This is not an exhaustive list but merely an indication of the types of conduct that could come under the heading of inappropriate. Senior leaders will use their professional judgement to determine whether any act or behaviour not outlined on the list above is considered unacceptable use of our ICT facilities.

Exemptions from Unacceptable Use

Where the use of our ICT Facilities is required for a purpose that would otherwise be considered an unacceptable use, an exemption to the Acceptable Use policy may be granted where such an exception is required for our related business (such as lawful study or research). The requesting user should notify their Headteacher/ CEO or CEA (or Service Manager), prior to undertaking an unacceptable use, who must obtain explicit written permission for such use from the DPO or Head of ICT, as appropriate. Advice on the application of certain legislation as it applies to the use of IT can be sought from the DPO.

Remote Learning

Online collaboration is essential for remote learning providing increased opportunities to maintain the connection between school and home.

Users engaging, participating or otherwise connected to our ICT Facilities are expected to abide by our Digital and Data Acceptable Use Policy, and all other applicable policies, including but not limited to each school's Remote Learning Policy.

Visitors

Arrangements in relation to visitors are detailed within our Cyber Security Policy, available in the **All MAT Staff** area on Teams.

Encryption

Arrangements in relation to device encryption are detailed within our Cyber Security Policy, available in the **All MAT Staff** area on Teams.

ICT Monitoring

Access to our ICT facilities is provided for business purposes. To protect our legitimate business interests, we may monitor and/or record your email and instant messaging usage if:

- you are absent for any reason and communications must be checked to ensure business continuity is maintained;
- we suspect that you have been viewing or sending offensive, obscene, defamatory, discriminatory, intimidating, malicious, insulting or otherwise inappropriate or illegal material;
- we suspect excessive personal use;
- we suspect that you are sending or receiving emails that are detrimental to the Trust and/or in breach of data protection laws;
- we have grounds for suspecting criminal activity; or
- it is necessary to investigate a grievance or disciplinary matter.

When monitoring emails, we will, unless there are exceptional circumstances, confine ourselves to looking at the address and subject heading.

We may monitor and/or record your internet use if:

- we suspect that you have been viewing or sending offensive, obscene, defamatory, discriminatory, intimidating, malicious, insulting or otherwise inappropriate or illegal material;
- we suspect excessive personal use;

- we suspect that you are posting statements that are detrimental to the Trust and/or in breach of data protection laws;
- we have grounds for suspecting criminal activity, such as theft or fraud; or
- it is necessary to investigate a grievance or disciplinary matter.

Monitoring will consist of checking the websites that you have visited and the duration of such visits.

Breach of Policy

For staff, any breaches of this Policy will be managed under the Trust's Disciplinary Policy and Procedure, which can be located in the **All MAT Staff** area on Teams. Failure to follow this policy may also lead to criminal or civil action.

For pupils, any breaches of the Pupil Acceptable Use agreement will be managed under the relevant School's Behaviour Policy.

Appendix 1: Primary Pupil Acceptable Use Policy Agreement

We need to be safe when we use computers and the internet. To help us stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets;
- I will only use activities that a teacher or suitable adult has told or allowed me to use;
- I will take care of the computer and other equipment;
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong;
- I know that my school may look at my use of computers / tablets;
- I will not take pictures, or record something I see on the computers / tablet;
- I will tell a teacher or suitable adult if I see something that upsets me on the screen; and
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Name (child):

Signed (child):

Parent/Carer

I have read and understand that use of the Academy IT systems and devices is governed by the full Acceptable Use Policy and all of the policies available from the Academy's website: www.manormultiacademytrust.com

The Academy's systems and devices are primarily intended for educational use and must not be used for personal or recreational purposes unless expressly permitted. The Academy may monitor use of the systems, devices and digital communications at any time.

Parents and Carers should sign below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to the Academy's ICT Facilities.

Print Name (parent):

Signed (parent):

Date (parent):

Appendix 2: Acceptable Use Policy Agreement (Staff / All other adult users)

ICT is seen as beneficial to all members of the Academy in supporting learning, teaching, research, administration and approved business activities of the Academy. The Academy's ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the academy. This could also lead to breaches of the data protection rights of a number of individuals causing harm to those individuals, and to the Academy.

This Acceptable Use Agreement is intended to ensure:

- that all users, will be responsible and stay safe while using ICT devices, systems and services.
- that Academy devices, systems, services and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk.

Agreement

I understand that I must use Academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users, including as to the personal data of others.

When using the Academy's ICT Facilities:

- I understand that the Academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have prior permission;
- I understand that the Academy may monitor my use of the devices, systems, services and communications at any time;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will not disclose or share personal information about others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.…), unless expressly permitted by job description or in writing from the Academy;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);

- I will respect others' work and property and will not access, copy, remove or otherwise use or alter any other user's files, without the owner's knowledge and permission, and I will ensure that any use is in accordance with Academy policies;
- I understand there are risks when using the systems and services, and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will respect copyright of materials and intellectual property rights and not take or distribute text, images or other materials without permission;
- I will not use or modify any of the Academy devices, systems and services in any way that will disrupt their use for others in any way;
- I will not install or attempt to install or store programmes of any type on any Academy device, nor will I try to alter computer settings;
- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc.…) to any Academy devices, systems or services without prior permission from an Authorised Person within the Academy. I understand that, if I am permitted to use my own devices in the Academy I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Academy's policies. I will not use my personal equipment to record these images, unless I have permission from the Academy and from the individual to do so;
- I will only use social networking sites in school in accordance with the Academy's policies;
- I will only communicate with students, parents / carers, and other parties solely related to my employment, using systems authorised and provided by the Academy. Any such communication will be professional in tone and manner;
- I will not engage in any on-line activity that may compromise my professional responsibilities;
- I recognise that a failure to comply with the policies of the Academy, and any misuse of ICT equipment, could lead to breaches of the rights of data subjects and I will act at all times in accordance with such policies in order to avoid any inappropriate use of personal data, or the breach of the data protection rights of any individual.

I understand that I am responsible for my actions, both inside and outside of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (for example, use of images, digital communications, or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy ICT systems and services, disciplinary action as set out in the codes of conduct and in the event of illegal activities involvement of the police.

I agree to follow these guidelines at all times when:

- using or connected to the Academy's devices, systems and services;
- using my own equipment inside or outside of the Academy in a way that is related to me being a member of this Academy (for example, communicating with other members of the Academy, accessing Academy email, websites and services, etc.…).

I have read and understand that use of the Academy IT systems and devices is governed by the full Acceptable Use Policy and all of the policies available from the Academy's website www.manormultiacademytrust.co.uk

Print Name: _____

Signed: _____

Date: _____