THIS POLICY COVERS ALL ACADEMIES/SCHOOLS WITHIN ARDEN MULTI-ACADEMY TRUST

Name of Policy	**Staff Acceptable User Policy**	
Lead	Martin Murphy, CEO	
Governor Committee	Business & Personnel Committee	
Policy Status	Originally drafted	July 2012
	Trustee Approved	12th December 2023
Version No.	1	
Next Review	Autumn Term 2024	
Amendments	Andy Hinsley, June 2017 (minor amendment)	
	26th November 2019 – reviewed by Y Hennous – amendments to reflect GDPR regulations	

Guidelines for staff

Arden Multi-Academy Trust (the Trust, AMAT) has provided computers for use by staff as an important tool for teaching, learning, and administration of the Trust. Use of Trust computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the Trust's computer systems in a professional, lawful, and ethical manner. Deliberate abuse of the Trust's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the Trust's networks is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the Trust and staff, to safeguard the reputation of the Trust, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the Trust recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the Trust neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the Trust.

Computer security and data protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so, you will be required to change your password immediately.
- You **must not allow a pupil to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the Trust.
- You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the Trust.
- When publishing or transmitting non-sensitive material outside of the Trust, you **must** take steps to protect the identity of any pupil whose parents/carers have requested this.

- If you use a personal computer at home for work purposes, you **must** ensure that any Trust-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You **must not** make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the Trust) or a personal computer.
- You **must** ensure that items of portable computer equipment (such as laptops, i-pads, digital cameras, flip cameras or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Although equipment offsite is covered by the Trust's insurance, it does not cover the theft of an item in transit whilst the vehicle is left unattended unless specific security precautions have been complied with (see Insurance policy for specific details). Additionally there is (currently) a £500 excess on all insurance claims. In the event of loss or damage through carelessness or preventable theft, the employee will be liable for this excess or the cost of replacement equipment whichever is lesser. Employees may want, therefore, to ensure that they have adequate insurance cover of their own in place.

Personal use

The Trust recognises that occasional personal use of the Trust's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- **Must** comply with all other conditions of this AUP as they apply to non-personal use, and all other Trust policies regarding staff conduct;
- **Must not** interfere in any way with your other duties or those of any other member of staff;
- **Must not** have any undue effect on the performance of the computer system;
- **Must not** be for any commercial purpose or gain unless explicitly authorised by the Trust.

Personal use is permitted at the discretion of the Trust and can be limited or revoked at any time.

Use of your own equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be used until approved. This test must be performed at regular intervals as required by the Trust's normal rules on electrical safety testing.
- You must **not connect** personal computer equipment to Trust owned computer equipment without prior approval from IT Network staff, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the Trust computer system.

Conduct

- You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet
    - Excessive storage of unnecessary files on the network storage areas
    - Use of computer printers to produce class sets of materials, instead of using photocopiers
- You should avoid eating or drinking around computer equipment.
- In addition to the guidelines here, all use of the internet is governed by a legal agreement with our Internet Service Provider (ISP).

Use of social networking websites and online forums

Staff must take care when using social networking websites such as Facebook or Twitter, Instagram, etc., even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You **must not** add a pupil to your 'friends list'.
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should avoid contacting any pupil privately via a social networking website, even for Trust-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.
- You should regularly check and update your privacy settings on all social media sites and apps as they can be changed by companies without users realising.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the Trust – even if their online activities are entirely unrelated to the Trust.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the Trust.
- You should not post any material online that can be clearly linked to the Trust that may damage the Trust's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Further guidance on the use of social media for school and personal use is given in the Social Media Policy.

Use of email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the Trust. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the Trust via e-mail without proper authorisation.
- All Trust e-mail you send should have a signature containing your name, job title and the name of the school within the Trust.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the Trust.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The Trust will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of pupil use

- Pupils **must** be supervised at **all** times when using the Trust computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable User Policy for pupils is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the Trust computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the Trust to ensure compliance with this Acceptable User Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the Trust does keep a complete record of sites visited on the internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the Trust computer system that is unrelated to the Trust activities (such as personal passwords, photographs, or financial information).
- The Trust may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the Trust computer systems indicates your consent to the above described monitoring taking place.**

Confidentiality and copyright

- Respect the work and ownership rights of people outside the Trust, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the Trust computer systems or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You **must** consult a member of IT network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the Trust is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the Trust's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the

The Trust or capable of being used or adapted for use within the Trust shall be immediately

disclosed to the Trust and shall to the extent permitted by law belong to and be the absolute property of the Trust.

- By storing or creating any personal documents or files on the Trust computer system, you grant the Trust a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the Trust sees fit.

Reporting problems with the computer system

It is the job of the IT Network Manager to ensure that the Trust's computer systems are working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via the online Support Request system.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting breaches of this policy

All members of staff have a duty to ensure this Acceptable User Policy is followed. You must immediately inform a member of the IT network staff, or the Associate Headteacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within the Trust that you feel are unsuitable for staff or student consumption;
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- Any breaches, or attempted breaches, of computer security;
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the Trust computer system.

Reports should be made either via email or the online Support Request system. All reports will be treated confidentially.

Review and evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

1. "Sensitive personal information" is defined as information about an individual that is protected by law under the General Data Protection Regulation (GDPR) 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the Trust's Data Protection Policy.

See Appendix 1 (signature page)

Acceptable User Policy for students

I know that I must use the computers safely.

- I know that the Trust can remotely monitor what I do on the computers.
- I will treat my username and password sensibly – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online, and will not share personal information about myself or others.
- If I arrange to meet someone that I have communicated with online, I will do so in a public place and take an adult with me.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that the Trust will look after me and my classmates and can help if anything happens online – even if I am using a computer at home.

I know that I must use the computers responsibly.

- I will only upload pictures or videos from inside the Trust if I have permission.
- I understand that the Trust's security and Internet filter is there to protect me, and protect the computer network, and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.
- I will only download music or videos onto the computer if it is related to my Trust work.
- I understand that I must not download or display inappropriate pictures or other material from the internet.

I know that I must help look after the computers.

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the the Trust computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.
- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.
- I know that food and drink is not allowed in the computer rooms, and that I should not eat or drink around any computer.

I know that I must respect others when using the computers.

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.

- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.

See Appendix 1 (signature page)

Appendix 1

I, _____ [name] agree to abide by the Trust's Staff Acceptable User Policy.

Signature: _____

Department
(if not student): _____

Date: _____