ACCEPTABLE USE POLICY

Learning Academies Trust

Version:	2.0		
Approved by:	Finance & Personnel Committee	Ratified date:	12 May 2022
Last review date:	02 May 2022	Next review date:	01 May 2023

LEARNING ACADEMIES TRUST

CONTENTS

CHANGES

Policy date	Summary of change	Author	Version	Review date
23/04/2018	Policy has been created.	Luke Pollard, IT Operations Manager	1.0	23/04/2019
12/05/2022	Clarification around monitoring. Remove personal usage of work device. Change in handling of USB & passwords. Minor changes to wording and layout.	Luke Pollard, IT Operations Manager	2.0	12/05/2022

1. AIMS

Technology is integral to the operation of our schools, being used internally and externally to deliver our learning environment and other essential services to pupils, staff, governors, and guests. All users are entitled to safe access to the internet and digital technologies provided. This policy is intended to ensure:

1. All users will be responsible and stay safe while using the internet and all other technologies provided by Learning Academies Trust.
2. All users are protected from potential risk in their use of technology and any accidental or deliberate misuse that could put the security of the systems and users at risk.
3. All users understand that Learning Academies Trust monitors devices and user activity for safeguarding and security purposes.
4. All users understand their responsibilities to ensure that Learning Academies Trust is compliant with General Data Protection Regulation imposed by law.

Learning Academies Trust aim to ensure that all users will have good access to technology to enhance their work and/or learning opportunities and will, in return, expect users to agree to be responsible users.

2. ACCEPTABLE USE

Users understand that they must use school systems in a responsible way to ensure that there is no risk to their safety or the safety of others. Users must not use any technology in a way that could pose a risk to the security or availability of our systems. Users should recognise the value of technology within our organisation and treat all

users, equipment, and systems with respect and act diligently to ensure everyone has safe and uninterrupted access to our technologies.

Users understand that the rules set out in this agreement apply to the use of all technologies provided by Learning Academies Trust, and any bring-your-own-device (BYOD) being used to access any of our resources.

Usage

1. Users understand that digital technologies provided by Learning Academies Trust are intended for educational and operational use only and they must not use the systems for personal or recreational use.
2. Users must not use the Trust computing systems for storage of personal files or photos.
3. Users must not access, copy, remove, or otherwise alter any other user's files, without their express permission.
4. Users must not upload, download, or purposely access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), inappropriate, or may cause harm or distress to others. Users must not use any programmes or software that might allow them to bypass the filtering and security systems in place to prevent access to such materials.
5. Users must not use our computing facilities to access, generate, or manufacture illegal or pirated content.
6. Users understand that the printing facilities are strictly for business usage and that the facilities must not be used for personal printing. Users understand that Learning Academies Trust reserves the right to charge back the cost of any personal printing that has been printed/copied from their account.

Security

7. Users understand that Learning Academies Trust monitors and audits the technologies provided by the Trust for the purpose of safeguarding and security. The auditing and logging facilities will attribute actions and usage activities to individual user accounts. See the partial list below of current auditing and logging activities:
    1. Web traffic interception – lists the internet activity for each user and is used to filter internet access and flag for any content that may be deemed inappropriate or a safeguarding concern.
        1. This applies to all devices (personal or corporate) that connect directly to the Trust network.
        2. This also applies to all corporate owned devices with internet access external to the Trust network.
    2. Key logging – monitors your keyboard usage on Trust owned devices for any safeguarding concerns. Alerts are monitored by a team of safeguarding professionals who will inform the school of any serious concerns.
    3. Authentication auditing – lists any authentication attempts to our servers or cloud systems. This contains information such as your IP, device, location, username, and number of logon attempts and is used and analysed by security systems to monitor for suspicious activity and to proactively respond to security issues.
    4. Network auditing – tracks the devices connected to our wireless and wired networks. This provides the IP, device, device health, location, and username information. This information is used to secure our network and audit the location of devices.
    5. Print auditing – monitors both printing and photocopying jobs to allocate costs to the appropriate school and to ensure users are printing in compliance with this acceptable use policy.
    6. Email filtering – all incoming and outgoing emails are audited via the Microsoft 365 ATP service and checked for malware, phishing, data exfiltration, and more. These systems are crucial to our system security as most attacks will originate via a communication or malicious payload sent to our users.
    7. File access – our security systems have a behaviour monitoring solution that audits access to files. This information is looking for suspicious or malicious activity to track, prevent, and respond to security threats.

8. Password management:

    1. Users must not disclose their username or password to anyone else as it is their responsibility to keep this information private. Users should understand that auditing and logging information can be attributed to their account and any inappropriate, malicious, or illegal activity will be traced back to their account, for which they could be held liable.

    2. Users understand that passwords must be secure and randomly generated. Users must not use any sequential or easy/common passwords and where possible should use a long memorable passphrase. See https://support.learningat.uk/support/solutions/articles/51000005878 for guidance.

    3. Users should memorise their password or passphrase and should not write it down anywhere. The Trust reserves the right to remove or destroy any documentation that is visible or accessible containing their password.

    4. Users should understand that nobody (including our IT technicians) should ask for a copy of your password and they should refuse to provide a copy if asked.

        1. If a technician is performing remote support, they may ask you to enter your password to fix the issue you are having but will not need to retain a copy of your password. If you are ever unsure if this is a genuine, please call our helpdesk directly on 01752 938035 to check.

        2. On a rare occasion a technician may need access to your account to diagnose or fix an issue. In these circumstances the technician will reset your password with a temporary password whilst they resolve the issue and then you should reset the password again once they are done. Please note an authorised technician can reset your account password and you should never give your current password out.

    5. Users must never use another person's account and should always login to their own account.

9. Users understand that upon termination of their contract all access to Learning Academies Trust digital facilities will be disabled and they will be required to surrender any equipment belonging to the Trust.

10. Users must not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if they have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

11. Users must not install or attempt to install programmes of any type on a machine, store programmes on a computer, or alter computer settings without authorisation from the Trust's technical support team.

12. If users wish to use their personal devices (laptop / iPad / tablet / phone / etc.) within a school, they must only connect to the guest wireless network for internet access. Users must not connect their personal device to the core network under any circumstances.

13. Users will be required to enrol in Multi-Factor Authentication if they wish to use their accounts external to the Trust's network. This will require the user to register their account to an independent device using the Microsoft Authenticator app so they can authorise authentication requests.

Data protection

14. Users must only transport, hold, disclose, or share personal data about themselves or others as outlined in the GDPR policy. Any data that they have access to will be kept private and confidential, except when it is deemed necessary that they are required by law or by policy to disclose such information to an appropriate authority.

15. Users must immediately report any breaches of personal or confidential data to the Headteacher, Data Protection Officer, and the technical support team. Users understand the severity of such incident and that they must report the breach on the same day.

    1. The quicker users act on sharing information of a breach or a potential breach, the quicker our technical team can work to try and isolate and limit the damage or exfiltration of data.

    2. Should the breach be notifiable, the Trust is required by law to report the breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

16. Users must store and transfer information via their OneDrive folder (from a Trust issued account not a personal OneDrive), Sharepoint folder, or via a shared drive located on the school server. Users must not transfer any personal or sensitive data via portable media such as a USB hard drive or memory stick.

17. Personal or sensitive data shared via email must be encrypted using the secure email solution (OME) built into Microsoft Outlook.

18. Where the encryption of data cannot be facilitated, users must remove all personal and identifiable information from the original document before transferring the data.

19. Users must not sign up/create accounts to any online service for other users (pupils, staff, or governors) unless the service has been assessed and approved by the IT Operations Manager or Data Protection Officer.

    1. Learning Academies Trust are required by law to perform a GDPR privacy impact assessment on all third-party systems that store any personally identifiable information prior to their use.

Communications

20. Users must communicate with others in a professional manner and must not use aggressive or inappropriate language.

21. Users must only communicate with students, parents/carers, staff, or governors via official systems approved by the Trust. Communications from a personal device is strictly forbidden in situations where contact information (such as a phone number or email address) has been obtained from a school management system.

22. Personal contact information of users such as a mobile phone number or email address should not be shared with other users unless they have given express permission for that information to be shared. All users have the right to revoke the use of their personal contact information and other users shall be required to delete the contact information if requested.

23. Users should refrain from sending communications outside of working hours unless the communication is necessary. Users have the right to disconnect after working hours and will not be required to respond to any communications outside of working hours.

    1. If a user decides to work outside of hours, please consider the use of the 'delay send' function within Outlook so that the email gets sent in the following morning (or Monday if you are working on the weekend). This minimises the notifications sent to users outside of working hours.

    2. For users that use the Outlook app to access emails out of hours, you can click on the bell icon to mute notifications from your work account during the evenings and weekends.

24. Users must only use social networking sites in school in accordance with the school's e-safety policy and/or staff handbook.

25. Users must not engage in any on-line activity that may compromise their professional responsibilities.

Property

26. Users understand that Learning Academies Trust own the intellectual property of any documents or resources generated for the school during their contracted hours.

27. Users must not distribute any intellectual property belonging to Learning Academies Trust to any person or company outside of our academy without prior permission.

28. Users understand that whilst Learning Academies Trust takes great care to provide a secure and reliable system, the Trust is not responsible for the loss or destruction of any data belonging to them. If they bring their own device into school the Trust is not responsible in the event of loss, theft, or damaged to that device.

29. Users must not disable, or cause any damage to school equipment, or any equipment belonging to others.

30. Users must report any damage or faults to our technical support team immediately. Users must not allow a third-party company or individual to attempt a repair on a school issued device.

Compliance

31. Users must immediately report any illegal, inappropriate, or harmful material or incident they become aware of to the technical support team or other appropriate person.

32. Users must ensure that they have permission to use the original work of others in their own work. Where work is protected by copyright, users must not download or distribute copies (including music and videos) unless they have permission and have declared the usage on the school's copyright licensing form.

33. Users must ensure that when taking or publishing images of others they will do so with their permission and in accordance with the school's policy on the use of images/videos. Users must not use personal equipment to record these images/videos. Where they are published (e.g. on the school website) it will not be possible to identify by name or other personal information of those who are featured unless consent has been given.

34. Users must not use any personal accounts when viewing third party streaming service in school such as Netflix, Amazon Video, Disney+, etc. See https://support.learningat.uk/support/solutions/articles/51000005881.

3. AGREEMENT

Users should understand that if they fail to comply with this Acceptable Use Policy agreement, they could be subject to disciplinary action. This could include a verbal warning, written warning, a suspension, referral to Governors, referral to Directors and/or the Local Authority, and in the event of illegal activities the involvement of the Police.

By choosing the Accept button, you agree to all terms set out in this document. If you decline the terms, you will be unable to access any of Learning Academies Trust's digital systems. This could affect your ability to complete duties required in your employment contract.

You should be prompted to accept or decline the terms when you first log into your Learning Academies Trust issued account. If you are not being issued with an account, please complete and sign the form below instead. By signing the form below, you are agreeing to all terms set out in this document.

Print Name: _____

Signed: _____

Date: D D / M M / Y Y Y Y