ANGLIAN LEARNING

ICT POLICY

THIS POLICY WAS APPROVED:	AUTUMN 2023
POLICY VERSION:	4.2
THIS POLICY WILL BE REVIEWED:	AUTUMN 2024
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW:	DIRECTOR OF ICT
THIS POLICY WAS CONSULTED WITH:	TECHNICAL SERVICES TEAM EXECUTIVE LEADERSHIP TEAM
THIS POLICY WAS DISTRIBUTED TO:	TRUST LEADERSHIP GROUP CENTRAL LEADERSHIP TEAM ALL TRUST STAFF

Contents

Foreword

All Anglian Learning's Information Communication Technology (ICT) facilities, equipment and information resources remain the property of Anglian Learning and not that of specific individuals, teams or departments. By following this policy, the community can together help ensure that ICT facilities are used legally, securely, effectively, efficiently, without compromising the reputation of Anglian Learning and in the spirit of co-operation, trust and consideration for others.

This policy relates to all ICT facilities and services provided by Anglian Learning, although particular emphasis is placed on security and device, email and internet usage. All employees, volunteers, and any other users of the Trust's ICT facilities are expected to adhere to this policy.

There are separate documents that form the pupil/student Acceptable Use Policies, which are tailored to the different phases of their education and are overseen by the Trust Safeguarding Group.

1. Disciplinary measures

1.1. Deliberate and serious breach of the policy statements in this section may lead to Anglian Learning taking disciplinary measures in accordance with Anglian Learning's Disciplinary Procedure. Anglian Learning recognise that ICT facilities, especially internet access, email and other cloud services are valuable business tools. However, misuse of these facilities can have a negative impact upon students, employees and volunteer productivity, as well as the reputation of the organisation.

2. Security

2.1. Individual users of Anglian Learning's equipment and services are responsible for their activities.

2.2. Workstations should not be left unattended for any reason, for any length of time. Screens should be locked to prevent unauthorised access. Failure to do this, could lead to activities being undertaken in the user's absence, in their name.

2.3. No attempt should be made to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents.

2.4. Additional access to information or resources can be arranged through the appropriate channels, starting by contacting a member of the Technical Services Team.

2.5. The use of cloud software systems is now commonplace and Anglian Learning schools use a very broad range of such services.

2.5.1. The procurement of cloud services should only be undertaken by schools when in conference with the Trust IT Manager, who can advise on:

2.5.1.1. The suitability of the service from a GDPR perspective.

2.5.1.2. The practicality of implementing the system, including any wider system contexts that might need to be considered.

2.5.1.3. Whether the school or wider Trust already has a solution in place that might meet the need.

2.5.1.4. Whether other schools in the Trust also use the proposed system, which could lead to the potential for a more beneficial commercial agreement, given the economies of scale that can be achieved.

2.5.1.5. The best method of implementing and managing the system and to help identify key stakeholders who will take responsibility for the system once it is in production.

2.5.2. Single Sign-On (SSO) technology allows software providers to make use of a third-party service such as Microsoft 365 to authenticate a user logging in, instead of issuing a separate username and password. Whilst also being more convenient for the user, this is also more secure, as it allows the organisation to consistently apply additional layers of security, such as Conditional Access policies and Multi-Factor Authentication, as well as monitoring solutions to detect suspected rogue actors.

2.5.2.1. All online software used by Anglian Learning should utilise SSO technology by September 2025.

2.5.3. Cloud-based software services often require the population of data such as staff and pupil lists, class groups and other information, which is ultimately sourced from the school's Management Information System. Manual record keeping in such systems is not practical and should be avoided, as this can lead to out-of-date records being retained and this has the potential to lead to staff being able to access systems after their departure from employment. The Trust can support a variety of methods to enable the automatic management of records in such systems that are equipped to receive records in this way.

2.5.3.1. It is anticipated that systems that do not support this by September 2025 may no longer be suitable to use on the grounds of security, Safeguarding and GDPR compliance.

2.6. User password management.

2.6.1. Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else, even for a short period of time.

2.6.2. Passwords should be created such that they cannot be easily guessed by people who know the creator, or derived from public information; for example, on social media.

2.6.3. Whilst it is better than a straight word, replacing letters with numbers, for example a letter 'O' with a zero, has limited value, as these rules are easily exploited.

2.6.4. A good strategy is to use a passphrase and then abbreviate, whereby a sentence is created or chosen and turned into a string of letters. For example, "Baa baa black sheep have you any wool? Yes sir, yes sir, 3 bags full!" would turn into the password "Bbbshyaw?Ys,ys,3bf!" by using the first letter of each word and the punctuation as your password. This example should not be used in real life.

2.6.5. Passwords must be unique for corporate accounts and should not be reused for personal accounts or for other corporate systems.

2.6.6. Staff and governor passwords should be:

2.6.6.1. at least 12 characters in length; the longer, the better.

2.6.6.2. Considered ‘complex’, in that three of the four available character sets are used within the password. Character sets are Uppercase, Lowercase, Numbers and Symbols.

2.6.6.3. The previous 5 passwords a user has had in place cannot be reused.

2.6.7. Student passwords should be:

2.6.7.1. At least 8 characters in length; the longer, the better.

2.6.7.2. Need not necessarily use multiple character sets, but by adding complexity through the use of different character sets (Uppercase, Lowercase, Numbers and Symbols) can help make the account more secure, although length alone adds efficacy.

2.6.7.3. Delegated student password changing can be provided to school staff through ALIS User Management facility, which is a method to change passwords quickly in the classroom. Requests for additional personnel to be granted access to this should be submitted to Technical Services.

2.6.7.4. A new initial password structure for pupils/students is being introduced that takes the form [number] [adjective] [colour] [animal], providing a good degree of uniqueness, complexity and efficacy, whilst being memorable. Trust IT Managers are working with school leaders on this implementation.

2.6.7.4.1. These initial passwords for Primary school pupil accounts are limited to 4 characters per word, to improve access.

2.6.7.4.2. “Clever” badges are available on request for primary school or other pupils which allow password-less login using an image/webcam approach to authentication.

2.6.8. Passwords are not set to expire, as contemporary thinking is that a unique, complex password is more secure than one that regularly changes.

2.6.9. After 10 failed attempts to log in, the account is temporarily suspended for 10 minutes. The count of failed attempts is reset every 10 minutes. This helps guard against brute force attacks on an account.

2.6.10. Storing your passwords rather than trying to remember them is allowed. The Trust has 1 approved method below. Passwords should never be written down manually.

2.6.10.1. Use a password manager. These services allow you to easily create and maintain long, complex and unique passwords for every service you use. To help you choose a reputable product, please contact Technical Services.

2.6.11. Passwords can and will be reset if they are suspected to be compromised or weak. Users are also free to reset their passwords at their own discretion at any time using one of the following methods:

2.6.11.1. The password management facilities within Office 365.

2.6.11.2. The native Windows tool, using Ctrl-Alt-Del → Change Password.

2.6.11.3. The ADFS service: https://adfs.mat.uk.net/adfs/portal/updatepassword

2.6.11.4. Approaching a school colleague with access to the ALIS User Management suite with rights to change staff passwords.

2.6.11.5. Contacting helpdesk@anglianlearning.org.

3. Use of Email

3.1. When to use email:

3.1.1. Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

3.1.2. The use of Teams chats as an alternative to email can focus communications to specific subjects and of reduce email volume.

3.1.2.1. It should be noted that Teams chats, like Email, are subject to disclosure in the case of a Data Subject Access Request, under the General Data Protection Regulation legislation.

3.1.3. A phone call can be the best form of communication for urgent messages.

3.1.4. Trust policy for email use includes that users must:

3.1.4.1. comply with current legislation;

3.1.4.2. use email in an acceptable way;

3.1.4.3. not create unnecessary business risk to Anglian Learning by their misuse of the internet.

3.1.4.4. comply with any relevant school email Protocols.

3.2. Unacceptable use

3.2.1. Sending confidential information to external locations without appropriate safeguards being in place. See Section 5 of this document for more details.

3.2.2. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene, illegal, discriminatory, offensive or abusive, or the context constitutes a personal, sexist or racist attack, or might be considered as harassment or bullying.

3.2.3. Using copyrighted information in a way that violates the copyright.

3.2.4. Seeking to gain unauthorised access to any of the Trust's systems or that of another organisation's system.

3.2.5. Broadcasting unsolicited personal views on social, political, religious or other non-business-related matters.

3.2.6. Transmitting unsolicited commercial or advertising material.

3.2.7. Undertaking deliberate activities that waste employee effort or system resources.

3.2.8. Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

3.2.9. Forwarding corporate email to a personal account.

3.3. Data Protection

3.3.1. Always exercise caution when committing confidential information to email since the security of such material cannot be guaranteed. Anglian Learning reserves the right to monitor electronic communications in accordance with applicable laws and policies, including the Computer Misuse Act 1990 and the General Data Protection Regulation 2018. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within and outside the system as well as deleted messages.

3.3.2. Caution should be taken when using the Reply-to-all feature of email. It is not always appropriate for recipients to respond to everyone included in the initial email.

3.3.3. When forwarding emails, or including additional recipients in a reply, caution should also be taken. It is worth considering the impact of having these new individuals seeing not only the most recent message, but any of the messages in the historic chain of emails, which may also be included in this message.

3.3.4. Emails are included in Subject Access Requests that are made under Sections 7–9A of the Data Protection Act 1998 and the General Data Protection Regulation 2018. As such, staff should be aware that any reference to the names of individuals may result in these messages being disclosed to the subjects, should such a request be received.

3.3.4.1. Even where student initials are used, such messages can also be subject to disclosure.

3.4. Email etiquette, housekeeping and threat awareness

3.4.1. When publishing or transmitting information externally be aware that you are representing Anglian Learning and you could be seen as speaking on behalf of the organisation. Make it clear when opinions are personal. If in doubt, consult your line manager.

3.4.2. Professional language and manner should be maintained whenever sending emails.

3.4.3. Inboxes should be checked at regular intervals during the working day. Teachers should check at the beginning and end of the school day as a minimum.

3.4.3.1. Junk folders should be checked daily, as legitimate messages sometimes get inappropriately classified as spam.

3.4.3.2. Where received, personal spam reports from the email provider should be reviewed.

3.4.4. Electronic files only should be kept of electronic correspondence, with only necessary messages being retained. It is very rare that printing paper copies is necessary.

3.4.5. It is good practice to keep your inbox fairly empty, such that it only contains items requiring action. Certain actions are taken for each

message, e.g., deletion, reply, flagging it for later processing, saving the whole email in a folder, or extracting just the useful information and saving it somewhere suitable.

3.4.6. Treat others with respect and in a way in which you would expect to be treated yourself. For example, do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague.

3.4.7. Do not forward emails warning about viruses. Instead, submit them to the Trust's Cyber Awareness partner, FairPhish, using the PhishSOS button on Outlook. It can also be useful to take a screenshot of the message and send it through to the Technical Services Helpdesk.

3.4.8. Do not open an email unless you have a reasonably clear expectation of what it contains and do not download files unless they are from a trusted source. Alert the Technical Services Team if you are sent anything like this unexpectedly. Vigilance is one of the most effective protections against email-based attacks.

3.4.9. Periodic simulations of harmless pseudo-threat emails are run throughout the year and directed at staff inboxes. These non-judgemental exercises form a critical part of the Trust's security posture and help keep leaders appraised of the level of awareness within the organisation as a whole.

3.4.9.1. These simulations are complemented with tips via email, taking various forms and providing a steady supply of training and support to our community, which staff are strongly encouraged to engage with.

3.5. Email signatures

3.5.1. Keep these short and include your name, job title, phone number(s) and website address.

3.5.2. Avoid excessive use of imagery.

3.5.3. A confidentiality disclaimer is automatically added to all emails that are sent to external recipients.

3.6. Auto-responders

3.6.1. Auto-responder (or Out of Office) messages return an automatic reply to the sender to the first message sent to the recipient after it is switched on. This can be useful to alert any senders to the mailbox owner's absence from work.

3.6.2. Auto-responders can be set by individual users at any time, using Outlook or Outlook Online. Details of how to do this can be found in the Microsoft 365 Guidance for Staff and Governors on Connect.

3.6.3. Auto-responders can be applied for any brief period of absence and discretion should be used as to whether this is appropriate and necessary. Examples of use include those working part-time, or those with a high level of email traffic that often require time-critical responses.

3.6.4. Auto-responders are applied administratively during the summer holidays to all mailboxes that do not have one already scheduled.

3.6.5. Auto-responders are sometimes applied administratively during other holiday periods.

3.6.6. Auto-responders are applied to mailboxes when a member of staff leaves the organisation.

3.7. Communication with students and parents

3.7.1. Staff should use only official school email accounts when communicating with students, parents or otherwise acting on behalf of the school or Trust.

3.7.1.1. When contacting students electronically, only school-issued email, cloud service or other internal service accounts should be used and never through private accounts.

3.7.1.2. The use of WhatsApp and other private means of messaging should not be used to communicate with students or parents.

3.7.2. As the boundaries between the online and offline worlds blur, students may try to include staff in their 'friends' list on their online social networks, such as Tiktok, Snapchat, Instagram and Facebook, or obtain a personal email address or mobile number. Whilst this could be harmless, it is important that staff keep a professional distance online, just as they would in the offline world, and therefore:

3.7.2.1. Staff should not approve any students as 'friends', 'followers' or roles of equivalent terminology which enable access to otherwise private content.

3.7.2.2. Student leavers should not be added or approved as connections for a period of 5 years after leaving school.

3.7.2.3. Staff should delete any existing connections with students in Social Media contexts.

3.7.2.4. Staff should remain aware that students can set up false identities and pose as others those known to them and so should exercise caution accordingly when approving Social Media connections.

3.7.3. Personal email addresses, mobile numbers, social networking IDs and other such information must remain strictly private.

3.7.4. Email or telephone communications between staff and a student that are deemed to fall outside agreed Trust guidelines may lead to disciplinary action or a criminal investigation.

4. Use of the Internet

4.1. Use of the Internet by employees and volunteers is permitted and encouraged where such use supports the goals and objectives of the school or Trust.

4.2. However, whilst using the Internet, employees and volunteers must ensure that they:

4.2.1. comply with current legislation;

4.2.2. use the internet in an acceptable way;

4.2.3. do not create unnecessary business risk to the organisation by their misuse of the internet.

4.2.4. understand that the corporate connection is both filtered and monitored.

4.3. Unacceptable behaviour

4.3.1. In particular the following is deemed unacceptable use or behaviour by employees and volunteers (this list is non-exhaustive):

4.3.1.1. Downloading or uploading materials which contain obscene, hateful, violent, pornographic, homophobic or would fall into other categories that may be considered inappropriate for the intended use of the access or are illegal in nature;

4.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

4.3.1.3. Using the internet to send or post offensive or harassing material to other users;

4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

4.3.1.5. Hacking into unauthorised areas;

4.3.1.6. Creating or transmitting defamatory material;

4.3.1.7. Undertaking deliberate activities that waste employee's effort or networked resources, including the use of any form of Denial-of-Service attack.

4.3.1.8. Deliberately or recklessly introducing any form of computer virus into Anglian Learning's network.

4.3.1.9. Writing, publishing, searching for, bookmarking, accessing or downloading material that might be regarded as obscene or pornographic.

4.4. Copyright

4.4.1. Care should be taken to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.4.2. Be aware of copyright law when using content you have found on websites. The law is the same as it is for printed materials.

4.4.3. The use of private streaming services, such as Netflix, Amazon Video and Disney Plus should only be made in cases where the specific content has been approved by the provider for educational use. The majority of material provided by these services do not come with rights for such use.

5. Confidentiality

5.1. When dealing with personal, sensitive and / or confidential information, extra care must be taken to protect the information.

5.2. Whilst screen sharing in an online meeting, or whilst extending screens to a display in a classroom or meeting room, due care should be taken to ensure that private or confidential information is not displayed to inappropriate audiences.

5.3. Whilst sharing a camera feed in an online meeting or lesson, care should be taken to ensure that the surrounding area around the view is appropriate, particularly when in a domestic context. Use of privacy filters is encouraged, in packages that support this, such as Teams, Google Meet and Zoom.

5.4. If communicating personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the personal nature of the information being sent, or the appropriate level of protection that might be required, please seek advice from the school's GDPR lead, a member of SLT or Technical Services staff.

5.4.1. Personal, sensitive and / or confidential information should not be sent by email attachment unless absolutely necessary. In cases where it is necessary, appropriate steps must be taken to encrypt the file or the whole message, with no exceptions. Guidance on this can be found in the Microsoft 365 Guidance for Staff documentation on Connect.

5.4.2. A more secure way to communicate data is via a OneDrive shared document.

5.4.3. External domains with which sharing can occur are curated by Technical Services. Any new recipient domains must be allow-listed within Microsoft 365 before this is possible. Please note that it can take several hours to take effect after a change is applied, so advance notice is advised, where possible.

5.4.4. Any password or key to an encrypted file or message must be sent separately; and ideally communicated by another means e.g., telephone, text message.

5.4.5. Before sending the email, verify the recipient by checking the address, and if appropriate, telephone the recipient to check and inform them that the email will be sent.

5.4.6. Never send sensitive information to personal email accounts; only ever use corporate accounts for this. Examples of personal email domains are @gmail.com, @outlook.com and @yahoo.co.uk. Corporate domains usually refer to the organisation within them in some way.

5.4.7. Do not refer to personal details in the subject of the email.

5.4.8. Never send an email that contains even encrypted personal data in haste. Always take time to ensure that the recipients are correct and that the data content is not broader than intended. For example, check unlabelled spreadsheet tabs if the document originated from another user.

6. Document Management

6.1. All data should be stored within the corporate systems of Anglian Learning, which are secured using enterprise-class security principles. Examples of acceptable locations are the Anglian Learning tenancies of Microsoft 365 and Google Workspace, local file shares as other systems that are secured using an Anglian Learning account.

6.2. Organisational documents should not be stored on private devices, unless these are of a public nature, such as those published on public websites.

6.3. The use of the Trust's cloud storage facilities is not permitted for private use.

6.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (e.g., you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space, can introduce unnecessary Data Protection risk and may cause confusion over version control.

6.5. Documents should be organised into a suitable folder structure and efforts should be made to delete content that is no longer relevant, particularly when it contains personal data.

6.6. Anglian Learning have a multi-threaded approach to data backup.

6.6.1. For staff using the OneDrive client on managed laptops or desktops, data stored in the Documents, Pictures and Desktop folder is backed up automatically to Microsoft 365.

6.6.2. Microsoft 365 and Google Workspace data is backed up daily to a third-party service, extending the retention of backups from the default offered within these services and providing a degree of resilience against the unavailability of these services.

6.6.3. Centralised on-site services are backed up daily to three separate storage solutions, one of which is "locked" in an immutable state, providing further resilience against ransomware attacks.

6.6.4. Legacy school systems are also backed up, using a variety of methods ranging from tape backup to cloud service and follow the standards-based 3-2-1 rule.

6.7. USB storage devices have traditionally been used to move data from one computer to another. Once encrypted, these can store information safely from a data protection perspective, but even these can still, inadvertently, transport threats into a network. This can lead to the severe disruption to services and even widespread data loss. As such, these devices are only permitted for use by exception, as assessed by the Technical Services Team.

6.7.1. Where portable / removable storage devices are used, these should be encrypted, unless there are sound technical reasons why this is not possible and in such cases, data stored should not feature personal details.

6.7.1.1. Restrictions are in place that limit the use of portal / removable devices due to the possibility of ransomware and other threats entering the network via this route, as well as the risk of data breaches.

6.7.2. Office 365 and Google Workspace offer very flexible methods of storing and sharing information and are the modern successor to portable USB storage. Files can be downloaded from these services or shared via secure links. Even so, it is understood that there are certain circumstances in which USB storage devices would be the natural choice for moving data. Various scenarios are described below, with new guidance shared for each circumstance.

6.7.2.1. Some tasks require increased storage requirements. An example of this would be video editing where you would need to use and store large video files. In these circumstances, access to an external hard drive to expand storage would be supported. These external hard drives would need to be encrypted and allow-listed by the Technical Services Team.

6.7.2.2. Most handheld cameras (not including smartphones) store photos on an SD card which would then be used to access the photos from another device. Photography and videography can be supported via the Technical Services Team. SD cards will need to be stored in a locked drawer/cupboard/safe when not in use and is the responsible user's role to ensure this happens.

6.7.2.3. It remains common for external guests to use USB sticks to bring in media for presentations/interviews. Guests should instead be encouraged to have these media files stored within their own cloud platform, in advance of their visit. It would also be acceptable for guests email the files to their contact at the school, or send them as secure links. If these approaches are not practical, the Technical Services Team can advise further.

6.7.3. Devices for the purposes of examinations can be provided by Technical Services. There will be two ways in which this would be approached:

6.7.3.1. The provision of laptops that are connected to our school network but cannot access the internet and are locked down by policy. In these cases, work will be saved into a network location that can be accessed by authorised users.

6.7.3.2. Completely offline devices with no access to the network or internet. In these cases, a specially prepared USB stick would need to be used. These would be secured by Bitlocker and set to automatically unlock without a password on approved devices. Unapproved devices would require a password to access the storage device.

7. Personal use of ICT facilities

7.1. Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. These include websites such as Instagram, Facebook, X (formally known as Twitter) and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and be aware that this is a constantly evolving area.

7.1.1. Use of Social Media at work

7.1.1.1. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from Anglian Learning's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

7.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

7.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee [or volunteer]. It is, therefore, imperative that you are respectful of the organisation's service as a whole, including clients, colleagues, partners and competitors.

7.1.1.4. Employees and volunteers should not give the impression that they are representing, sharing opinions or otherwise making statements on behalf of Anglian Learning unless appropriately authorised to do so. Personal opinions must be acknowledged as such and should not be represented in any way that might make them appear to be those of the organisation. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of Anglian Learning.'*

7.1.1.5. Any communications that employees or volunteers make in a personal capacity must not:

7.1.1.5.1. bring Anglian Learning into disrepute, for example by criticising clients, colleagues or partner organisations;

7.1.1.5.2. breach the Anglian Learning's policy on client confidentiality or any other relevant policy;

7.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

7.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

7.1.1.5.5. use social media to bully another individual;

7.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

7.1.2. Anglian Learning maintains the right to monitor usage where there is suspicion of improper use.

7.2. Other personal use

7.2.1. Use of facilities for leisure or personal purposes (e.g., sending and receiving personal email, personal phone calls, playing computer games and browsing the internet at appropriate times) is permitted so long as such use does not:

7.2.1.1. incur specific expenditure for Anglian Learning;

7.2.1.2. impact on the performance of your job or role (this is a matter between each member of staff or volunteer and their line manager);

7.2.1.3. break the law;

7.2.1.4. bring Anglian Learning into disrepute;

7.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

7.2.1.6. impact on the availability of resources needed (physical or network) for business use.

7.2.2. Any information contained within Anglian Learning in any form is for use by the employee or volunteer for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of a member of Technical Services Staff.

7.3. Take note of the points relating to Social Media within Section 3.7 (Communication with Students) of this policy.

7.4. Any users who place and pay for orders online using personal details do so at their own risk and Anglian Learning accepts no liability if details are fraudulently obtained whilst the user is using Anglian Learning's equipment.

8. Staff Equipment

8.1. This section covers items such as managed laptops and mobile devices. Please refer to section 6.7 of this policy when considering storing or transferring personal or sensitive data.

8.2. All activities carried out on Anglian Learning's systems and hardware are subject to monitoring, to Safeguard members of the Trust's community.

8.2.1. You may find, in your role, that you have access to electronic information about the activities of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g., to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

8.2.1.1. In the case of a specific allegation of misconduct, the Headteacher or CEO, with advice from the Director of People and the Director of ICT, or nominated deputies, can authorise accessing of information for the

purposes of investigating the allegation.

8.2.1.2. When use of the device is considered concerning by any monitoring software in place, such as in relation to internet searches, whereby a screenshot is logged and reviewed by nominated senior staff.

8.2.1.3. Accounts may be accessed for operational reasons, such as in the case of a leaver, or long-term sickness leave, maternity leave or other long period of absence. Where a member of staff remains employed by the Trust, consent from the employee would be sought in the first instance.

8.2.1.4. A member of Technical Services may unavoidably access detail whilst working on systems. In this case, the use of any information gained will be restricted to undertaking the administrative task in hand.

8.3. Employees and volunteers must ensure that all data belonging to Anglian Learning is stored on Anglian Learning's network (or cloud service, such as Microsoft 365) and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

8.4. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

8.5. All staff laptops are domain joined and encrypted, which renders the hard drive inaccessible if removed (having been lost or stolen), without the necessary security keys.

8.6. Rooms with computer equipment in should not be left unsecured. Classrooms should be locked if a device is to be left unattended.

8.7. Ensure that all locally stored data, including diary entries, are synchronised regularly with the appropriate enterprise storage solution, such as OneDrive, on a frequent basis.

8.8. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades, as requested by the Technical Services Team.

8.9. The addition of any software applications to Anglian Learning computers must be fully licensed, authorised by a member of Technical Services Staff and documented in the Anglian Learning Software Licensing Register. The installation should be carried out by the same team, or by the primary user with their approval.

8.10. Portable equipment must be transported in a protective case where one is supplied.

8.11. Portable equipment taken out on long-term loan by staff, such as laptops, are subject to the Anglian Learning Portable Device Loan Agreement. This document must be signed by the member of staff or parent (for students), ahead of taking possession of the equipment and a copy retained by both parties.

8.12. Users requiring the installation of any form of additional hardware onto devices managed by the organisation should seek guidance from the Technical Services Team, who reserve the right to refuse such request if, in

their assessment, it could cause conflict to existing hardware, be incompatible or otherwise cause undue operational impact.

8.13. Where damage is caused to staff devices which has most likely occurred due to neglect or failure to follow this policy will be rectified through shared liability for the costs between the home department of that member of staff and ICT budgets.

8.14. It is not permitted to rearrange the way in which equipment is plugged in (computers, phones, printers, network cabling etc.) without first contacting a member of the Technical Services Team. Network points are configured to perform a specific function and documented as such. Moving devices between ports may not have the anticipated effect, but will disorder documentation and may cause service disruption at that time or in the future.

8.15. Food and drink should be kept away from equipment and not consumed nearby.

8.16. Anglian Learning does not operate a formal Bring Your Own Device policy, as hardware is provided to staff whose roles require such equipment. However, Guest WIFI is available and can be used for internet access purposes by visitors and others only requiring access to web services. Internally hosted systems are not accessible via this service and no Trust data should be stored on such devices.

9. Remote Access

9.1. The cloud systems operated by Anglian Learning are accessible whilst on the school site, but also whilst at home or elsewhere from school-issued, managed devices.

9.2. Personal mobile phones may be used to access Microsoft 365, Google Workspace and other cloud systems, but are subject to the following conditions.

9.2.1. Devices should be kept up to date using the vendor's operation system software, such as iOS (Apple) and Android (used by Samsung) etc. Mobile phones that are out of support should not be used to access Trust systems.

9.2.2. Devices should be secured using a PIN, or better still some form of biometric authentication, such as facial or fingerprint recognition.

9.2.3. Copies of files, attachments etc. should not be downloaded to or stored on these devices.

9.2.4. Where the use of such devices is shared with family members or other persons unrelated to the Trust, any applications used to access Trust systems should have additional securities in place, such as a biometric challenge upon the launch of a related application.

9.2.5. All profiles relating to Trust systems should be removed from the device on or before the last day of employment with Anglian Learning.

9.2.6. In the event of a personal device being lost or stolen, the Technical Services Team should be notified and a remote sign-out and wipe of work-related accounts will be initiated.

9.3. Accounts within Microsoft 365 are secured using Conditional Access policies, such that:

9.3.1. Staff and Governors using Microsoft 365 or any system federated to it using Single Sign-On technology, within the UK, but outside of an Anglian Learning school network are subject to Multi-Factor Authentication.

9.3.1.1. Students in this same circumstance are not required to operate Multi-Factor Authentication due to related practicalities.

9.3.2. Access to Microsoft 365 or any system federated to it using Single Sign-On technology outside of the UK is possible by arrangement only for all user groups. Requests providing the anticipated dates of travel can be submitted to the Technical Services Helpdesk for scheduling.

9.3.3. Access to Microsoft 365 or any system federated to it using Single Sign-On technology whilst on any Anglian Learning school site is accessible via password only and not subject to Multi-Factor Authentication.

9.3.3.1. Global Administrators of Microsoft 365 are subject Multi-Factor Authentication from any source.

9.3.4. The Multi-Factor Authentication policy supports three forms of token delivery:

9.3.4.1. The Microsoft Authenticator app (preferred method)

9.3.4.2. SMS (text message)

9.3.4.3. Telephone call

9.4. Some staff may, on occasion, have need to remotely access services hosted within the Trust's network. The school's Trust IT Manager can advise on the best option in each case. Remote access to internal systems must only be undertaken from Trust-managed devices and not personal computers.

10. Accessing support from the Technical Services Team

10.1. The Technical Services Team is available to provide support and advice on any matter relating to ICT use within Anglian Learning. As an initial point of contact, please email helpdesk@anglianlearning.org. When raising a ticket, it can help you receive a timely and complete response by bearing the following in mind:

10.1.1. Any member of staff can communicate directly with the Technical Services Team and need not necessarily communicate through another colleague.

10.1.2. Be clear, with relevant detail about the matter you are raising.

10.1.3. Include any steps that would allow the team to recreate the problem you are experiencing.

10.1.4. Open a single ticket for each matter being raised.

10.1.5. Add any extra detail to the same ticket. This is easy to do through the Halo Helpdesk Portal, to save searching through emails.

10.1.6. Provide additional information when requested.

10.1.7. Inform the team, ideally via the ticket, when a matter can be closed.

10.1.8. It helps to reopen related tickets if the same issue re-arises, rather than creating new ones.