ANGLIAN LEARNING

ICT POLICY

THIS POLICY WAS APPROVED:	SPRING 2020
POLICY VERSION:	1.1
THIS POLICY WILL BE REVIEWED:	SPRING 2021
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW:	DIRECTOR OF IT
THIS POLICY WAS CONSULTED WITH:	
THIS POLICY WAS DISTRIBUTED TO:	ACADEMIES LEADERSHIP GROUP

Contents

The need for a policy

All Anglian Learning's information communication technology (ICT) facilities and information resources remain the property of Anglian Learning and not of particular individuals, teams or departments. By following this policy we will help ensure that ICT facilities are used:

- legally;
- securely;
- without compromising the reputation of Anglian Learning;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- efficiently.

The policy relates to all ICT facilities and services provided by Anglian Learning, although special emphasis is placed on email and the internet. All employees, volunteers, and any other users of our IT are expected to adhere to the policy.

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 accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees and volunteer productivity and the reputation of the organisation.

1.2. In addition, all of the organisation's phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

2. Security

2.1. As a user of Anglian Learning's equipment and services, you are responsible for your activity.

2.2. Do not disclose personal system passwords or other security details to other employees (including Technical Services), volunteers or external agents, and do not use anyone else's log-in; this undermines the security of Anglian Learning. If the security of your password is compromised, ensure that you change it or approach a member of Technical Services Staff to help you.

2.3. If you intend to leave your PC or workstation unattended for any reason, for any length of time, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away.

2.4. Any pen drives or other removable storage devices used on Anglian Learning's network should be secure and only those that are the property of Anglian Learning should be used. Please see paragraph 7 for more detail.

2.5. Do not attempt 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. If you do not have access to information or resources you feel you need, contact a member of Technical Services Staff.

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. When creating passwords make sure they can't be guessed by people who know you, 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 you choose or create a sentence and turn it 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 production, as should now any highly popular sentence structures such as song lyrics).

2.6.5. Passwords must be unique for your work accounts; do not reuse any password you have used for personal accounts or previous employers.

2.6.6. Passwords should be at least 12 characters in length; the longer the better.

2.6.7. Passwords must be considered 'complex', in that three of the four available character sets are used within the password. Character sets are Uppercase, Lowercase, Numbers and Symbols.

2.6.8. The previous 5 passwords a user has had in place should not be reused.

2.6.9. Storing your passwords rather than trying to remember them all is allowed. We have 1 approved method below. Passwords should never be written down manually.

2.6.9.1. 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.

2.6.10. 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.

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. Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees and volunteers of Anglian Learning is permitted and

encouraged where such use supports the goals and objectives of Anglian Learning.

3.1.3. Anglian Learning has a policy for the use of email whereby employees and volunteers must ensure that they:

3.1.3.1. comply with current legislation;

3.1.3.2. use email in an acceptable way;

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

3.1.3.4. comply with any relevant school email Protocols.

3.2. Unacceptable behaviour

3.2.1. Sending confidential information to external locations without appropriate safeguards in place. See paragraph 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 or illegal.

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

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

3.2.5. Seeking to gain unauthorised access to any of Anglian Learning's or another organisation's system.

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

3.2.7. Transmitting unsolicited commercial or advertising material.

3.2.8. Undertaking deliberate activities that waste employee's effort or networked resources.

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

3.3. Confidentiality

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. See paragraph 5 for more detail.

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 see not only your most recent message, but all of the messages in the historic chain of email, which may also be included in what you are sending.

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 shared with the subjects, should such a request be received. Where appropriate, student initials should be used rather than full names.

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

3.4. General points on email use

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

3.4.2. Check your inbox at regular intervals during the working day. Teachers should check at the beginning and end of the school day as a minimum.

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

3.4.2.2. When received, personal spam reports from the email provider should be reviewed.

3.4.3. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary.

3.4.4. It is good practice to keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

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

3.4.6. Do not forward emails warning about viruses (they are invariably hoaxes and Technical Services Staff will probably already be aware of genuine viruses – if in doubt, contact them for advice);

3.4.7. Do not open an email unless you have a reasonably good 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

3.5. Email signatures

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

3.5.2. Avoid excessive use of imagery.

3.6. Communication with Students

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

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

3.6.2. 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 Snapchat, Instagram and Facebook, or obtain a personal email address or mobile number. This could be harmless but it is important that staff keep a professional distance online, just as they would in the offline world, and therefore:

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

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

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

3.6.2.3. 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.

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

3.6.4. 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.

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.

4.3. 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 employees 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.

4.4. Chat rooms / instant messaging (IM)

4.4.1. The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed with your line manager.

4.5. Webmail

4.5.1. The use of personal webmail is not permitted in the organisation unless it has previously agreed with your line manager or occurs during a period of rest or whilst off duty.

4.6. Obscenities / pornography

4.6.1. Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

4.7. Copyright

4.7.1. Take care 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.

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

5. Confidentiality

5.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

5.2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please seek advice from a member of Technical Services Staff.

5.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

5.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

5.2.3. Any password or key must be sent separately; and preferably communicated by another means e.g. telephone, text message.

5.2.4. 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;

5.2.5. 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. If in doubt, seek advice from a member of Technical Services.

5.2.6. Do not refer to the information in the subject of the email.

6. Anglian Learning Network

6.1. Keep master copies of important data on Anglian Learning's enterprise network and not solely on your PC's local C: Drive or portable disks. Not storing data on Anglian Learning's network means it will not be backed up and is therefore at risk. Examples of acceptable locations are internal network shares, Anglian Learning accounts based on Google G-Suite and Office 365.

6.2. Ask for advice from a member of Technical Services Staff if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

6.3. Be considerate about storing personal (non-Anglian Learning) files on Anglian Learning's network.

6.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. 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 might cause confusion over version control.

7. Removable media

7.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must first contact Technical Services Staff for permission, but

7.1.1. Always consider if an alternative solution exists. Examples are use of a VPN, or an Anglian Learning account on a cloud storage solution, namely Google G-Suite or Office 365.

7.1.2. Only use recommended removable media.

7.1.3. Encrypt and password protect.

7.1.4. Store all removable media securely.

7.1.5. Removable media must be disposed of securely by Technical Services Staff.

8. Personal use of ICT facilities

8.1. 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. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

8.1.1. Use of Social Media at work

8.1.1.1. 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.

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

8.1.1.3. 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.

8.1.1.4. Employees and volunteers should not give the impression that they are representing, giving 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.'*

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

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

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

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

8.1.1.5.4. 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;

8.1.1.5.5. use social media to bully another individual;

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

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

8.2. Other personal use

8.2.1. 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:

8.2.1.1. incur specific expenditure for Anglian Learning;

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

8.2.1.3. break the law;

8.2.1.4. bring Anglian Learning into disrepute;

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

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

8.2.2. 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.

8.3. Take note of the points relating to Social Media within Section 3.6 (Communication with Students) of this policy.

9. Portable and Mobile ICT Equipment

9.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data.

9.2. All activities carried out on Anglian Learning's systems and hardware will be monitored in accordance with the general policy.

9.3. Employees and volunteers must ensure that all data belonging to Anglian Learning is stored on Anglian Learning's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

9.4. 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.

9.5. Synchronise all locally stored data, including diary entries, with the appropriate enterprise storage solution on a frequent basis.

9.6. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

9.7. 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 and the installation carried out by the same team, or by the primary user with their approval.

9.8. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

9.9. Portable equipment must be transported in a protective case if one is supplied.

9.10. 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, ahead of taking possession of the equipment and a copy retained by both parties.

9.11. 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.

9.12. Damage caused to school devices that, in all likelihood could not have been achieved by accident will be chargeable to the individual, where appropriate evidence can be produced.

10. Remote Access

10.1. If remote access is required, you must contact a member of Technical Services Staff to set this up.

10.2. You are responsible for all activity via your remote access facility.

10.3. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

10.4 To prevent unauthorised access to Anglian Learning's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

10.5. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

10.6. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

10.7. Protect Anglian Learning's information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-office environment.

10.8. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

10.9. Care should be taken when working on laptops in public places (e.g. trains) that any employee or client details are not visible to other people.

11. Electronic monitoring

10.1 You may find that you have access to electronic information about the activity 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:

10.1.1 In the case of a specific allegation of misconduct, when the Headteacher (or CEO for Trust Central staff) with advice from the Director of HR can authorise accessing of such information when investigating the allegation;

10.1.2 A member of Technical Services may unavoidably access detail whilst fixing a

problem, but use of any information gained will be restricted to finding and resolving the issue in question.

12. Online purchasing

10.2 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.

11 Care of equipment

11.1 Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, printers, network cabling etc.) without first contacting a member of Technical Services Staff.

11.2 Food and drink should be kept away from equipment and not consumed in close proximity to it.

Agreement

All employees, volunteers, contractors or temporary employees who have been granted the right to use the Anglian Learning's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	
Manager:		**Employee /volunteer:**	
Date:		**Date:**	