AMBITIONS
Academies Trust

ICT ACCEPTABLE USE POLICY

SCOPE:	Trust Policy
AUTHOR/ORIGINATOR:	Paul Holman
NAME OF RESPONSIBLE DIRECTOR/PRINCIPAL:	Business Director
APPROVING COMMITTEE:	Trust Board
STATUTORY BASIS:	General Data Protection Regulations, KASIE, Ofsted Framework, Academies Handbook
REQUIREMENT TO PUBLISH ON WEBSITE:	No
DATE CONSULTED ON BY JCNC:	N/A
DATE RATIFIED BY APPROVING COMMITTEE:	July 2020
REVIEW PERIOD:	Annually
DATE DUE FOR NEXT REVIEW:	July 2021
REFERENCE NUMBER:	To be added by Trust
ADDED TO ALCUMUS BY:	To be added by Trust
DATE DISTRIBUTED/ADDED TO ALCUMUS:	To be added by Trust

Outstanding Achievement for All

Contents:

Statement of Intent

Ambitions Academies Trust (AAT) promotes the use of technology and understands the positive effect it can have on enhancing pupils' learning and community engagement. However, AAT must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Academy Principal or the Trust's Data Protection Officer (DPO) as appropriate in order for any necessary further action to be taken.

This ICT Acceptable Use Policy is designed to outline staff responsibilities when using technology, whether this is via personal devices or academy devices, on or off the Trust's premises, and applies to all staff, volunteers, contractors and visitors.

AAT's intention in publishing an ICT Acceptable Use Policy is not to impose restrictions that are contrary to AAT's established culture of openness, honesty and integrity. The Trust is committed to protecting the employees and stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.

The policy will be monitored and evaluated regularly considering any incidents which occur or technological developments which might lead to a change in policy.

1. Introduction:

This policy applies to all employees, volunteers, supply staff and contractors (the user) using the Trust's ICT facilities.

The ICT Acceptable Use Policy is divided into the following three sections:

- general policy and code of practice
- internet policy and code of practice
- email policy and code of practice

This policy should be read in conjunction with the Data Protection Policy.

2. General Policy and Code of Practice:

The Academy and the Trust have well-developed and advanced ICT systems for the benefit of all users.

This policy sets out the rules that must be complied with to ensure that the system works effectively for everyone.

Privacy

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the Trust and the academies store on their networks regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

The Trust and its academies will only process data in line with their lawful basis to uphold the rights of pupils, staff and other third parties.

In order to protect pupils' safety and wellbeing and to protect the Trust from any third party claims or legal action against it, the Trust may view any data, information or material on the academy's or AAT's ICT systems (whether contained in an email, on the network, or device) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The Trust's privacy notice details the lawful basis under which the Trust is lawfully allowed to do so.

The disclaimer that automatically appears at the end of each Academy and AAT email notifies the recipient that any email correspondence may be monitored. This disclaimer **must not** be removed.

General Code of Practice:

The Academy's philosophy	In using ICT, the user will follow the academy's ethos and consider the work and feelings of others. The system **must not** be used in a way that is unprofessional or that might cause loss of service to other users.
Times of access	The ICT systems will be available 365 days a year, 24/7. However, to ensure the systems are kept up-to-date, there will be periods of time where scheduled maintenance is required. The ICT team will plan this with the Principal and endeavor to do this when the least impact will be made to working schedules.
User ID, password and logging on	The user will be given an ID and password. The user must keep these private and not tell or show anyone what they are. Passwords should: • Be a minimum length of 12 characters • Contain characters from three of the following four categories: o English Uppercase (A-Z) o English Lowercase (a-z) o Base-10 digits (0-9) o Non-alphanumeric characters (e.g. !$#%) If the password is forgotten or accidentally disclosed to anyone else, the user must report it immediately to a member of the ICT support staff. The user must not use another person's account or allow another person to use their account. The facilities are allocated to the user on a personal basis and they are responsible for the use of the machine when logged on. The academy's system records and senior ICT staff monitor the use of the system. Use of the academy's facilities by a third party using the user's username or password will be attributable to the user and the user will be held accountable for any misuse. The user must not log on to more than one computer at the same time.
Printing	The academy may wish to check that expensive resources are being used efficiently and the Principal or Line Manager may suggest other strategies to the user to save on resources.
Logging off	The user must log off from the computer they are using at the end of each session and wait for the standard login screen to reappear before leaving. The user must lock the computer if they move away from the screen. This signals to the system that the user is no longer using the service; it ensures security and frees up resources for others to use.
Access to information not normally available	The user **must not** use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. The user **must not** attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.

Connections to the system	The user must not connect any hardware which may be detrimental to the academy's network.
Connections to the computer	The user must use the keyboard, mouse and any headphones provided. The user **must not** attempt to use any of the connectors on the back of any desktop computer where accessible ports on the front are available. The user **must not** use USB memory sticks or other portable storage media for reasons of data security and GDPR compliance. All staff have access to Office 365 storage which allows the secure sharing of files with internal or external recipients. If the user wishes to use additional hardware with academy devices this must be checked with the ICT department for more support.
Virus	If the user suspects that their computer has a virus, ~~s/he~~ they must report it to a member of the ICT staff immediately.
Installation of software, files or media	The user **must not** install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. The user **must not** alter or re-configure software on any part of the academy's system.
File space	The user must manage their own file space by deleting old data rigorously. If the user believes that they have a real need for additional space, this should be discussed with a senior member of the ICT support staff.
Transferring files	The user may transfer files to and from their network home directories using AAT provided on-line services via Office 365 only. When transferring files to and from the user's network home directories, they **must not** import or export any material unless the owner of that material expressly permits the user to do so.
Reporting faults and malfunctions	The user must report any faults or malfunctions in writing to the ICT support staff, including full details and all error messages, as soon as possible via the Academies dedicated helpdesk email address or if not possible, via telephone call to the helpdesk.
Copies of important work	Any data containing personal and special category data **must not** be stored on unencrypted media. The ICT systems do keep backups of files stored in the user's home directory and shared area for a limited period of time, however, the ICT team are not responsible for any loss of data.

3. Internet Policy and Code of Practice:

The Trust and the academies can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.

Whenever accessing the internet using the Trust's or personal equipment the user **must** observe the code of practice below.

This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the Trust's facilities and information being damaged.

Any breach of this policy and the code of practice will be treated extremely seriously and it may result in disciplinary or legal action.

The Trust may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the Trust incurs because of the breach of this policy and code of practice.

Why is a code of practice necessary?

There are four main issues:

- Although the ICT facilities are often perceived as 'free', there is a significant cost to the Trust for using it. This cost includes support, staffing, subscription costs and the computer hardware and software.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle and to protect the staff and pupils who access the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the Trust or academy's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the academy on disks or other storage media.

Internet Code of practice:

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. The user may use the internet for other purposes provided that: • such use is occasional and reasonable. • such use does not interfere in any way with their duties. • the user always follows the code of practice.
Inappropriate material	The user **must not** use the internet to access any newsgroups, links, list-servers, web pages or other areas that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils.

	The user is responsible for rejecting any links to such material which may appear inadvertently during research. If the user encounters any material which could be regarded as offensive they **must leave that website or service immediately** and not make any copy of that material. If the user encounters an offensive or inappropriate website or service, they must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	The user **must not** misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the academy maintains a record which identifies who uses the facilities and the use that is made of them. The information collected includes which websites and services the user visits, how long the user remains there and which material is viewed. This information will be analysed and retained and it may be used in disciplinary and legal proceedings.
Giving out information	The user must not divulge any information concerning the Trust, the academies, its pupils or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the academy's name and your own name when accessing a service which the academy subscribes to.
Personal safety	The user must take care who they correspond with. The user **must not** disclose where they are or arrange meetings with strangers they are in contact with over the internet.
Hardware and software	The user **must not** make any changes to any of the academy's or AAT's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the academy and AAT are an important part of the security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the academy's systems.
Copyright	The user should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. The user must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits it.

4. Email Policy and Code of Practice:

The use of email, both within the Trust and with the wider community, is an essential means of communication. Email offers significant benefits including direct written contact between all layers of the organisation.

Users need to understand how to style an email in relation to good network etiquette. In the context of the Trust or the academy, emails should ***not*** be considered private and staff should assume that anything they write or email could become public. Therefore, they should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any data exchanged with an external agency must comply with Trust's Data Protection policy and GDPR principles. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or dismissal.

Code of practice

Purpose	All staff are given their own email account to be used as a work-based tool. The email account must be used for all business to minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal contact information being revealed. **Under no circumstances** should staff contact students, parents or conduct any academy business using any ***personal*** email addresses.
AAT's disclaimer	AAT requires a standard disclaimer to be attached to all email correspondence – "This email and any attachment to it are confidential, intended for the recipient only and should not be used without the permission of Ambitions Academies Trust. Unless you are the intended recipient, you may not use, copy or disclose either the message or any information contained in the message. If you are not the intended recipient, you should delete this email and any copies and notify the sender immediately. Ambitions Academies Trust cannot accept liability for any damage sustained as a result of software viruses. You should ensure that it is virus free before opening it. Think before you print!." The academy's email disclaimer is automatically attached to all outgoing emails and you must not cancel or disapply it.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form). For the safety and security of users and recipients all mail is filtered and logged by AAT's ICT support provider and if necessary, email histories can be traced. Principal, senior and ICT staff are entitled to have read-only access to your emails.

Security	It is the responsibility of each account holder to keep their password/s secure and to use their designated AAT email account so that it is clear who the originator of the message is. As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, the staff member must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email. There are also more phishing scams targeting businesses, so if the staff member receives an email that they believe to be fraudulent, let a member of the ICT team know and they can advise on how best to deal with it. **If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies follow guidance "Emailing personal, sensitive, confidential or classified information" which is detailed below.**
Program files and non-business documents	The staff member **must not** introduce program files or non-business documents from external sources on to the academy's or AAT's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the academy. If the staff member has any reason for suspecting that a virus may have entered the academy's system, they **must** contact the ICT support staff immediately.
Quality	Emails constitute records of the academy and are subject to the same rules, care and checks as other written communications sent by the academy. All external emails, including those to parents, should be constructed in the same way as a formal letter written on academy letter headed paper (ie. use of Dear, Mr/Mrs/Ms). Staff members should consider the following when sending emails: • whether it is appropriate for material to be sent to third parties; • the emails sent and received may have to be disclosed in legal proceedings or a suspicious activity report; • whether any authorisation is required before sending; • the confidentiality between sender and recipient; • transmitting the work of other people, without their permission, may infringe copyright laws.
Inappropriate emails or attachments	If a staff member receives any inappropriate emails or attachments they must report them to the ICT staff. • Keep the number and relevance of email recipients, in particular those who are being copied in, to the minimum necessary and appropriate.

	• Do not send whole academy emails unless essential for academy business. • Do not send or forward attachments unnecessarily. Wherever possible, send the location path to the shared drive rather than sending attachments. • Staff members **must not** send personal or inappropriate information by email about themselves, other members of staff, pupils or other members of the academy community. Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libellous, malicious, threatening or contravening discrimination legislation or detrimental to the recipient is a disciplinary offence and may also be a legal offence.
Viruses	Never open attachments from an untrusted source. If the staff member suspects that an email has a virus attached to it, they **must inform** the ICT staff immediately. This email ***must not*** be opened.
Spam	Staff **must not** send spam (sending the same message to multiple email) without the permission of senior staff.
Storage	Staff are advised to regularly delete emails that are no longer required and to organise emails into folders and carry out frequent house-keeping on all folders and archives. Old emails may be deleted from the academy's server after 12 months.
Message size	Staff are limited to sending messages with attachments which are up to 20Mb in size. Distribution of files within the academy can done by using shared areas.
Confidential Emails	Staff must ensure that confidential emails are always suitably protected. If working at home or remotely, they should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required. Emails created or received as part of a staff member's role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

5. Email Policy – Advice to Staff:

Staff should be guided by the following good practice:

- All emails should be written and checked carefully before sending.
- Check emails regularly.
- Respond to emails in a timely fashion. A holding email should be sent as soon as possible and responded to within three days.
- Activate "out of office" notification when away for extended periods.
- The setting to automatically forward and/or delete emails is not allowed. Individuals are required to "manage" their accounts.
- If any issues/complaints are involved then staff sending emails to parents, external organisations, or students are advised to cc. their line manager/s and other relevant individuals.

It is recognised that, during the week, staff work different hours to reflect personal circumstances. However, to support staff's work life balance staff they are encouraged, where possible, not to send emails:

- from 7pm Friday until Monday morning 7am on a normal working week;
- during half term, from 7pm on the day in which the academy closes for the holiday until the 7am the morning the academy re-opens;
- during the Christmas, Easter and Summer holidays, from 7pm of the day the academy closes until 7am of the morning it re-opens.

An exception to this is the need to support public examination results for students in the Secondary Sector including Tregonwell Petersfield Campus.

- During the summer holiday, from 7pm of the day the academy closes until the day prior to the exam results being received, no emails should be sent. Between the day prior to the GCSE (and A Level results) until the third day after the results, emails may be sent. Following this, emails should not be sent until the day that the academy reopens.

Further Guidelines:

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what is said to be taken, and it is easy to convey the wrong impression.
- Remember that sending emails from an academy account is similar to sending a letter on academy letterhead, so don't say anything that might bring discredit or embarrassment to yourself, the academy or the Trust.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

6. Confidentiality:

Members of staff will ensure the confidentiality, integrity and availability of their device systems at all times.

No personal data will be shared between staff and pupils via email.

When emailing parents or pupils, the BCC function will be used to protect the email addresses of others.

Staff members are not permitted to let their family members or friends use any Trust or Academy equipment which contains personal data – any member of staff found to have shared personal data without authorisation may be dealt with in accordance with the Disciplinary Policy and Procedures.

Staff will not verbally disclose personal data over the phone in the presence of an unauthorised person.

For further information or to clarify any of the points raised in this policy please speak to the Data Protection Officer (DPO).

All Staff, Trainees, Volunteers, Members, Trustees and Academy Committee Members need to read and sign a copy of the ICT Acceptable Use Agreement (AUA) to confirm they have read and understood the ICT Acceptable Use Policy.

ICT Acceptable Use Agreement (AUA) for Staff, Trainees, Volunteers, Members, Trustees and Academy Committee Members

All Staff, Trainees, Volunteers, Members, Trustees and Academy Committee Members with access to Ambitions Academy Trust (AAT) sites or computer devices, services and networks to sign an Acceptable Use Agreement (AUA), which outlines how we expect them to behave when using them, both in and out of academy.

This AUA is reviewed annually, and it is a requirement to sign it upon entry to the Trust and every time changes are made (usually also annually). **It is not exhaustive.**

All computer equipment, services and network access are intended to enhance professional activities, including teaching, research, administration and management. This agreement forms part of the Trust's ICT Acceptable Use Policy and has been drawn up to protect all parties - the students, the staff, the Academy and the Trust.

Agreeing to the terms of this agreement is a condition of use. Access to computer equipment, services and networks will form a condition of employment or engagement with Ambitions Academies Trust.

The Trust reserves the right to examine or delete any files that may be held on its computer systems or cloud services; or to monitor electronic communication and internet sites visited for the specific purpose of safeguarding.

I agree to the following terms:

a) Access to any device, network or cloud service must only be made via my authorised account and password, which must not be made available to any other person;

b) I will ensure the security of any device, network or cloud service I use, by locking devices with a password when unattended;

c) All internet use should be appropriate to professional activity or students' education;

d) Activity that threatens the integrity of the Trust's ICT systems, or that attacks or corrupts other systems, is forbidden;

e) Use of cloud and email services provided by the Trust for private interests, including personal financial gain, gambling, political purposes or advertising, is forbidden;

f) I am responsible for the email and instant messages I send and for adhering to the professionalism expected of all colleagues in our Email Policy;

g) When communicating electronically including the use of social media, I will behave in a positive manner, not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the Trust, Academy or teaching profession into disrepute. This applies both to public pages and to private posts;

h) Use of personal devices onsite, is controlled and any use should be limited and represents a consent to monitoring;

i) I must treat pupil data (including images of them, reports and safeguarding information) in strictest confidence and will not create, store or transmit it unless encrypted and viewable only by those with a legitimate professional reason, or as otherwise directed by the Data Protection Policy;

j) Appropriate images and videos of pupils and their work may be taken on a personal device in a group setting only by permanent staff, where parental consent for the purpose exists and an Academy device is not available, so long as they are deleted as soon as reasonable (including any automatic backups);

k) I will ensure in advance that any material I obtain or display from the internet to students is appropriate for the audience, especially when bypassing filtering, and necessary to an educational purpose;

l) Copyright of materials and intellectual property rights must be respected;

m) I understand that all activity using the Trust's devices, services and networks may be filtered and monitored without further warning.

n) If am allocated a device with specific permission to remove it from site, I will:

   i) Take reasonable care to protect it from data loss and physical loss or damage;
   ii) Be the sole user (not family) when offsite;
   iii) Only allow colleagues to use it with their own login;
   iv) Return it to the Trust Office or Academy when requested, after reasonable notice;
   v) Use it for professional purposes connected with education only;
   vi) Recognise that the device remains subject to routine monitoring;
   vii) Recognise that the device remains the property of the Trust at all times.

Academy name: _____

Full name: _____

Position: _____

Signed: _____ Date: ____/____/20____

Please sign two copies of this Acceptable Use Agreement.

Return a copy to the Trust or Academy Administration Lead and retain a copy for your own record.