ICT Acceptable Use Policy and Procedure

December 2022

Table of Contents

Introduction

1. Clarification

Where there are references to Ambitious about Autism in this policy, it is referring to both Ambitious about Autism (AaA) and Ambitious about Autism Schools Trust (AaAST). The policy must be implemented by both organisations.

Policy

1. Purpose and Scope

Granting Information & Communication Technology (ICT) access to staff to perform their job functions carries certain responsibilities and obligations which requires an understanding of what constitutes acceptable use of the Ambitious about Autism (AaA) corporate IT & Telephony infrastructure, IT network, and IT equipment. This includes any and all Audio Visual, Video Conferencing and Interactive Whiteboard equipment across the estate.

This policy explains how Ambitious about Autism's (AaA's) ICT resources are to be used and which actions are not allowed. Whilst this policy is as comprehensive and complete as possible, no policy can cover every situation. Questions as to what is deemed acceptable use can be directed to any member of the IT Team, the IT Helpdesk, the Executive Leadership Team (ELT), the Leadership Team of either TreeHouse School or The Rise School or the Leadership Team of Ambitious College, including the Whittington Supported Internship base room.

The Acceptable Use Policy (AUP) gives guidance to staff, contractors and volunteers on the behaviours and use of technology which are approved by AaA.

Since inappropriate use of the organisation's resources exposes AaA to various types of risk, it is important to specify what is permitted and what is not. The purpose of this policy is to detail the acceptable use of the organisation's ICT resources for the protection of all the parties involved.

Other policies to be referred to:

- Data Security Policy
- Data Protection Policy
- Confidentiality Policy
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- Child Safeguarding and Protection Policy and Procedure
- Adult Safeguarding and Protection Policy and Procedure
- Prevent Policy
- Relevant local IT and data policies in each school and college.

The use of computers and network resources is subject to meeting all relevant UK legislation including, but not limited to:

- Computer Misuse Act (1990)
- Regulations of Investigative Powers Act (RIPA) (2000)
- Freedom of Information Act (2000)
- Data Protection Act (2018) & General Data Protection Regulations (GDPR)
- Obscene Publications Act (1964)
- Copyrights, Design and Patents Act (1988)
- Communications Act (2003)
- Computer Copyright Software Amendment Act (1985)

2. Guidelines for Managers & Individuals

AaA's ICT facilities are provided for business purposes. The ICT AUP is a set of rules that applies to all authorised users of AaA's ICT facilities. ICT facilities are provided to staff and other authorised users primarily for AaA's business purposes to support teaching, learning, research and professional & administrative activities.

The scope of this policy includes all use of AaA's ICT facilities including but not limited to:

- Network infrastructure: including the physical infrastructure whether wired or wireless, network servers, networked storage devices, firewall, connections (cabled, wireless and remote) switches and routers.
- Network services; including internet access, email, wireless and networked file access & storage, cloud-based access & storage.
- Computing hardware including desktop computers, laptops, mobile devices, printers, monitors, keyboards, pointing devices, audio visual equipment and video conferencing equipment.
- Software and Databases including applications and information systems, video conferencing environments and software tools.

Bringing the policy and other relevant data security/protection policies to the attention of users

Staff are informed of the AUP policy at core induction. It is also the responsibility of the appropriate Executive Leadership Team (ELT) member or their nominated delegate to ensure that the policy is brought to their attention.

All users of the ICT facilities must comply with the following:

- AaA expects staff to use the ICT facilities in a responsible manner in accordance with its policies and current legislation. Please refer to Section 1 of the policy for relevant UK legislation / AaA policies to be referred to.
- Keep passwords, usernames and identities issued to you for whatever purpose confidential. This includes not sharing these details with colleagues, even for work purposes.
- Use MFA (Multi-factor Authentication) across supported systems (such as Office 365) when logging into or accessing AaA systems from outside of the organisation, when available, or required to do so.
- Store documents appropriately either on SharePoint, Microsoft Team sites, or in the user-specific, allocated OneDrive location. Each and every member of staff has access to a OneDrive storage location specifically intended for storage of documents and files pertaining to their work. All users are expected to use these designated storage areas so as to ensure their files and documents are routinely protected and backed up as well as to increase security. Users should refrain from long-term storage of documents on the desktop of any computer they use.
- Treat any information that becomes available to you as confidential, unless it is intended for unrestricted distribution, without explicit permission from the person or department entitled to give it.
- Take all reasonable precautions to ensure the security of ICT resources with passwords where possible.
- Use good information security and management practices for the storage, access, retention, and deletion of AaA data or information.
- Seek written authorisation from an appropriate ELT member or their nominated delegate for any work activities requiring access to prohibited internet material where the work may conflict with the AAA Acceptable Use Policy or legislation. Such occurrences should be exceptional.
- Comply with copyright legislation, licences and agreements for software and electronic information resources when connecting to AaA ICT resources.
- Consult with the IT Team staff to obtain appropriate software licences when required. All software should only be installed by an authorised employee, or with the express permission of a member of the IT Team.

- Make all reasonable efforts not to open emails or email attachments from unsolicited or untrusted sources.
- Notify a member of the IT Team if you suspect your computer or mobile device is infected with a virus or its security otherwise compromised.
- Be aware that AaA business purposes (primary purpose) of ICT facilities take priority over any personal use.
- Ensure personal use is occasional, reasonable and does not go against the primary purpose of the facilities; interfere with, conflict with or take priority over the performance of AaA duties; waste resources; deny service to or have a negative impact on staff or other authorised users.
- Access to the internet and social networking resources for personal use should generally be restricted to before 8.30am, after 17.00hrs and between 12.15 and 13.45hrs. AAA, however, appreciates that a work / life balance is important, so a reasonable, balanced approach to personal use of company internet resources should be applied in this area.
- Ensure that any computer located off site which is used to access AaA ICT facilities or services has regularly updated operating systems and anti-virus programs thereby protecting AaA from accidental or premeditated virus and hacking attempts and attacks. Non AaA equipment should be limited to accessing and maintaining AaA systems and data within the hosted environment only.
- Report technical problems, requests or concerns regarding a suspected policy breach to any member of the IT Team, or appropriate ELT member or their nominated delegate.
- Any and all AAA IT equipment should be periodically “shut down”, so as to allow internal maintenance tasks and software updates and upgrades to take effect.
- All external storage devices, including USB pen drives and hard disks, are automatically blocked from use with AaA PC’s and Laptops. The IT Department as the ability to enable specific devices at request.

3. Inappropriate Use

Staff and authorised users may not use AaA ICT facilities to do the following (this list is not exhaustive but includes):

- Act in a manner that is not consistent with the professional status of AaA, misrepresents or brings AaA into disrepute.
- Deliberately or intentionally access, create, change, store, download or transmit;
  - Any illegal or indecent images or videos, data or other material except for the purposes of properly authorised, supervised, lawful and authorised research.
  - Any infected material or malicious code designed specifically to be destructive to the normal or correct operation of computer systems, software, networks, data storage and/or other data, or attempt to avoid any precautions taken to prevent such damage.
  - Any material that AaA may view to be advocating illegal activity, such as copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, radicalisation, forgery, impersonation etc.
  - Any material that infringes the copyright of another person or institution or infringes UK copyright laws and other countries (including but not exclusive to music, films, radio and TV programmes).
- Before publishing any images of children or young people publicly, all staff should confirm that relevant permissions have been obtained by checking with the External Affairs team.
- Place links to websites that have links to or display inappropriate material or which facilitate illegal or improper use, or where copyright protected material such as computer software, music or any other copyrighted materials or media are unlawfully distributed.
- Gain unauthorised access to facilities or services via the AaA network.
- Allow, incite, encourage or enable others to gain unauthorised access to or carry out unauthorised access or modification to AaA’s ICT facilities.
- Change, damage, corrupt, deny, dismantle or destroy any ICT facility, network component, equipment, software or data, or its functions or settings owned by AaA.
- Under no circumstance should any non-AaA equipment including USB sticks be used on the AaA system without being scanned. Refer to the Data Security Policy for further information.

- Install any software not licensed by/to AaA or unauthorised copies of software on the AaA network under any circumstances.
- Distribute, transmit, disclose any AaA sensitive or confidential information to a third party.
- Staff must not open any email believed to be suspicious. It is the responsibility of staff to report any suspicious email to any member of the IT Team.
- Staff must not send email on behalf of another person or impersonate another user when sending email, unless authorised e.g., an EA on behalf of an ELT member.

4. Mandatory Prevention, Detection, and Investigation of Misuse

Periodic monitoring in some situations of email, internet use or other ICT usage may be carried out, if authorised by an ELT member or their nominated delegate, for the purposes of:

- Preventing and detecting criminal activities
- Investigating unauthorised use
- Establishing compliance with regulatory standards and Ambitious about Autism policies
- Ensuring effective system operation
- Any monitoring will be proportionate to the assessed risk to the ICT infrastructure and information systems. Tools used to protect AaA's infrastructure may include the use of the filtering software to limit browsing to inappropriate sites, downloads, automatic scanning of email and attachments for viruses
- AaA reserves the right to inspect any items of AaA owned computer equipment connected to the network. Any ICT equipment connected to the AaA network can be removed from if it is found to be breaching policy or otherwise interfering with the operation of the network.

5. Passwords

- Staff or other authorised users will be allocated a unique user login identity and a password for access to the AaA network. If accessing AaA systems from outside the organisation, multi-authentication may be required.
- Where a default password is allocated for first access, it must be changed immediately.
- A username or variation of a username should not form part of a password.
- Passwords must not be based on personal information (e.g., family names, pets, name of your street, car registration numbers, telephone numbers).
- Passwords must not be chosen from a dictionary.
- Staff or other authorised users must use their own and only their own username and must keep their passwords secure.
- As a guide, passwords should be at least eight characters long and consist of both alpha and numeric characters. Be strong e.g., choose one or two lines of a phrase, song or poem and use the first letter from each word followed by a number. e.g., Always look on the bright side of life generates a password "alotbsol77". Special characters such as '! # $' add additional complexity. Please note that some AAA systems may have quite specific password requirements.
- A password must be changed immediately through the relevant system password change function if a member of staff suspects it has been compromised. If the IT Team suspect an account has been compromised and are unable to confirm this with the related member of staff, then the IT Team will immediately force change the suspected password to maintain system security.
- Unattended computers must be either locked by use of the lock screen command on the windows security menu or completely logged out.
- Multi Factor Identification must be used in conjunction with passwords when the system being accessed requires users to do so.

6. Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, sensitive documents, personal information or credit card or financial details by disguising as a trustworthy entity in an electronic communication.

AaA staff must please ensure that when they are logging onto AaA systems, especially when outside of the organisation's settings, schools, or colleges, that they are logging on using a legitimate login page.

Some of these fake or fraudulent webpages often, but not always, originate from links within e-mails. Occasionally, these fake pages can look quite convincing. Equally, AaA staff should treat all e-mail from an unfamiliar source with due caution and not click on any links if in any doubt as to the precise purpose of that link.

Similarly, AaA staff should be extremely vigilant when logging on, and if any logging on or sign in page looks suspicious or you do not recognise the layout or configuration of the page, check with the IT Team before logging on or clicking on any links.

Whilst working from home computers is acceptable within this policy, staff should as a rule, be primarily working from the computer issued to them, and should not access AaA systems via public access computers. Examples of such computers would be computers in Internet Café's or Public Libraries. For security purposes AaA runs Microsoft 365 policies that enable some restricted functionality for home computers, contact the IT department for further information.

If at any time you feel you have inadvertently entered your login details, (username & password) into an illegitimate webpage, change your password if you are able to, and notify the AaA IT Team immediately.

7. Mobile Working

Technology used to support mobile working including laptops, tablets, mobile phones should be kept secure and password protected at all times. Any loss of a mobile device must be notified immediately to the IT Team or ELT member.

Any documents, which are stored on laptops, or other mobile devices must be routinely reviewed and deleted, as necessary.

8. Sanctions

AaA considers this policy to be extremely important. If a member of staff is found to be in breach of it, they may be subject to the AaA disciplinary procedure.

In certain circumstances, breach of this policy may be considered to be gross misconduct. AaA reserves the right to take legal action against individuals who cause it to be involved in legal proceedings or reputational damage as a result of their improper use of the AaA IT infrastructure or equipment, violation of licensing agreements and/or other contraventions to the policy.