ACET

EMPOWERING ACHIEVEMENT ● STRIVING FOR EXCELLENCE ●

ACET E-SAFETY POLICY
A policy for the acceptable use of Trust ICT Equipment

DOCUMENT CONTROL			
Policy Level	Trust (Junior & Senior)		
Approved by	Trust Board		
Approved Date	25TH July 2023		
Next Review Date	June 2024	**Frequency**	Annually
Business Lead	Network Manager	**Author**	Matthew Sutton
Version Number	**Date Issued**	**Updated Information**	
1.1	17/05/23	Revised entire policy. Linked to 4 C's of Safeguarding. Extracted Social Media advise and created separate policy. Consolidated legal guidance from all elements of the policy into a dedicated section.	

Contents

1. Purpose

The ICT systems and services of Aston Community Education Trust ("the Trust") form a vital element of operations, and as such must be protected as far as possible from any form of disruption or interruption to service.

Additionally, the more we rely on technology to collect, store, and manage information, the more vulnerable the organisation is to severe security breaches. Human errors, malicious attacks and system malfunctions not only cause great financial damage but also affect business continuity, compromise our GDPR compliance and can adversely affect our reputation.

It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for the Trust and its academy's needs. This policy sets out the measures and instructions to preserve our ICT systems and data, as well as everyone's responsibility to ensure our ICT systems and ICT equipment remain secure.

2. Scope

The Trust recognises that threats to systems may arise both internally and externally, and that malicious actors may target employees to gain systems access. The provisions in this policy apply to mitigate the risk posed by threats both inside and outside of the Trust network control.

This Policy covers all employees, contractors, volunteers and any other users of ICT who have permanent or temporary access to the Trust's ICT systems or data. Other relevant documents are the Staff Acceptable Use Policy (Appendix 2). For the purposes of this Policy, an ICT system means any device used for storage and the processing of data.

3. Policy Principles

The ICT Security Policy includes the requirements of the current legislation relating to the use of ICT systems, which comprise principally of:

- GDPR and Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988

It is important that all users are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action. Summary information relating to the legislation set out above is found in Appendix 1. In addition to this policy, the Trust's Data Protection Policy provides further guidance.

The Trust also has a Cyber Response Plan.

The E-Safety policy has been devised with the Trusts safeguarding approach in mind around online safety and the use of technology. The Trust has invested heavily in systems that address the 4 C's of risk: Content, Contact, Conduct & Commerce.

Trust web filters and firewalls are the first line of defence in preventing access to illegal, inappropriate or harmful content. They also prevent contact via the internet to known sites that may exploit or groom our young people and halt any risk of commercial exposure through online gambling, inappropriate advertising, phishing or financial scams. Any other harmful interaction using Trust technology which could compromise conduct should be captured using our preferred safeguarding solution Securus.

4. Policy Elements

4.1 Physical and Systems Security

4.1.1 Physical Equipment Management

Trust ICT assets and services are controlled by a centralised team. The Trust IT Services Team are responsible for the secure running of the Trust systems and services, and take all appropriate steps to ensure the confidentiality, availability, and integrity of these at all times.

Trust ICT assets are managed via an asset control register, with Senior ICT Technicians maintaining the register of assets per academy, and Trust central assets maintained separately. All hardware issued to end users should be traceable and end users are accountable for the condition of the equipment issued to them.

When equipment is issued that has access to the internet, security software which is fit-for-purpose should be present. This includes, but may not be limited to, anti-virus endpoint protection, a local firewall, and internet filtering software.

The following conditions apply when equipment is issued:

- only authorised personnel will have access to computer equipment
- only authorised software may be used on any computer equipment
- only software that is used for organisational or educational applications may be used
- no software may be brought onto or taken from the premises without prior authorisation from the Trust IT Services team
- before new software is introduced to the network it must be checked and authorised by the Senior ICT Technicians
- unauthorised access to the computer facility, unauthorised copying and/or removal of computer equipment/software, and any attempt to circumvent the software protections deployed by the Trust may result in disciplinary action.

Networking equipment, such as servers, switches and firewalls must be physically secure, in locked rooms and/or cabinets. Access to these systems must also be limited to prevent unauthorised access, and staff in the ICT team should have relevant training prior to access and carrying out changes.

No personal device should be connected to the core school or ACET network, instead utilising segregated networks such as Visitor Wi-Fi/BYOD, as the risk of unmanaged devices should not be presented to the internal school network.

All redundant IT equipment is disposed of ethically through a WEEE Waste registered company under the relevant legislation (detailed in the Legal Issues and Further Guidance section)

4.1.2 System Access Management

Systems access is granted by the Trust IT Services Team on the principle of least privilege, meaning that only the access required for a user to fulfil their role will be applied to a user account. This is reflected in the privileges assigned to the user object within Active Directory and Office 365.

Staff user accounts are created and disabled in a timely manner on receipt of notification from the Human Resources (HR) department, usually through an automated system. When receiving notification from the HR department that a member of staff is leaving or has left, in addition to the user account being disabled, any issued equipment will also be recovered.

Student user accounts are created and disabled automatically by the system, according to the data in the schools MIS. When a student is admitted at a school in the MIS, the system will create an account accordingly that night. When a student leaves a school and the MIS is updated to reflect this, the system will disable the account that night.

It is the responsibility of each school to determine the appropriate level of access to the various ICT systems in use, including Microsoft products, VPN access, the School’s MIS system and other software packages, as well as access to shared data resources such as local file servers and online collaborative resources such as Teams, SharePoint and

Google Workspace.

Responsibility for authorisation to the ICT systems lies with the Senior ICT Technician. In all cases, the Senior ICT Technician will be guided on authorisation requirements by HR and/or by line management as per above. Following a request being received, should there be any uncertainty about the suitability of a level of access this should be escalated to the Central ICT Trust management team and reviewed by the ACET Network Manager in conjunction with key stakeholders.

Any attempt, or complicity in an attempt, to circumvent the authorisation process for access permissions is a disciplinary offence, as is using the ICT facilities provided to in any way break the law. Examples of such breaches may include (but are not limited to):

- disclosing access credentials for information or services
- obtaining and using another user's details to access information or services
- making, distributing, or using unlicensed software or data
- making or sending threatening, offensive, or harassing materials
- creating, possessing, or distributing obscene material
- unauthorised private use of Trust's computer facilities.

4.2 Digital and Cyber Security

4.2.1 Device Protection

When staff use their digital devices to access information, such as email or files, they introduce risk to the security of the systems. We therefore require all staff to maintain security on devices used to access such systems by adhering to the following conditions:

- Ensure all devices are secured with a password, PIN, or biometric access process
- Ensure the presence of Trust approved anti-malware (including virus) software on any device
- Always ensure the physical security of devices (e.g. not left on display in a car)
- Only use secure networks to connect to Trust services (e.g. using a VPN if on public Wi-Fi)
- Never disclose or share passwords
- PCs and Laptops should always be locked when left unattended, and the screen turned off
- Staff should never share or loan their devices.

Any loss or new requirement should be raised with the ICT Team. This also applies if it is suspected that passwords or other credentials have been compromised.

Individuals will receive this policy on joining the Trust and should request clarification on any points they do not sufficiently understand.

4.2.2 Safe Use of Email

Malicious email is the primary vector of ingress to compromised networks. Therefore, good email discipline should be maintained around the use of the Trust's email systems and facility.

Good practises include (but are not limited to):

- Be suspicious of any email with an attachment or which includes links
- Verify the sender is as expected, and any attachment is also expected
- Check links are spelled correctly, and do not hide their true destination (hovering over link text should show the actual target)
- Never open any attachment, or click on any link, of which you are unsure
- Be wary of any email saying a file has been shared with you. Confirm this (verbally if possible) with the sender of the email
- Be wary of an email which says it contains a voicemail. Confirm this with ICT before clicking links or opening

Attachments

If a staff member is not sure that an email they received is safe, they must refer this to the Trust IT Services Department. Suspicious emails should never be forwarded as this can spread a virus.

4.2.3 Authentication Management (passwords)

Authentication integrity is a key component of the security of ICT Systems. This includes (but is not limited to) passwords, PIN codes, passphrases, biometric data and cryptographic certificates. In all instances these should be treated as highly confidential.

Strong discipline is encouraged when choosing authentication security. Wherever possible multi-factor authentication should be utilised to mitigate the risk of any one credential being compromised.

Passwords, PINs and passphrases should be as secure as possible, and should be memorable so as not to require the user to store this information in an accessible form anywhere.

Password length is a key to good security. For example:

"This is my passphrase and I remember it every day" is substantially more secure than "4^jsyR&f", due to the length as well as being easy to remember. Passwords should also be periodically reset in order to mitigate the risk of compromise and the Trust shall enforce this for staff.

4.2.4 Secure data transfer

Transferring data introduces security risk. It is, however, necessary (e.g., to exam boards). As such, Staff must:

- Avoid transferring sensitive data (e.g. pupil information, reports or marking sheets) to other devices or accounts unless necessary
- Only share confidential data over the Trust's network (including VPN) and not over public Wi-Fi
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- Ensure any email attachments containing personal or confidential data are encrypted and/or password protected, and ensure that the password to open an attachment is not included in the e-mail (ideally sent via a second channel such as SMS)
- Report scams, privacy breaches and hacking attempts.

In all cases the ICT Team will offer support if requested.

4.3 General Security Considerations

4.3.1 Backup and Recovery

The ICT Team ensure that backups of all ICT services and systems are taken regularly, and that checks are made to confirm the validity of the backup and restore process. This forms a component of the Disaster Recovery and Business Continuity policy, and the full process can be found therein.

4.3.2 Monitoring

The Trust and its schools have monitoring and recording systems in place, including a firewall, web filter, classroom management software such as Impero and Securus.

The CEO, Trust Executives, ACET Network Manager and Senior ICT Technicians reserve the right to monitor all email/internet activity by staff and students for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

Any investigation that relates to members of staff will not proceed without first having the authorisation of the CEO.

Issues discovered via monitoring software that relate to students are immediately reported to the Principal or Designated Safeguarding Lead, or in their absence, their Deputy DSL. Unless requested by the Principal / CEO, the ACET Network Manager will take no further steps regarding staff incidents. Should a matter arise that directly involves the Principal's / CEO's own use of the system, the matter will be referred by the ACET Network Manager to the Chair of Governors / Trustees as appropriate.

4.3.3 Firewalls and filtering

Regular procedures are in place for the ACET Network Manager and/or the Senior ICT Technicians to check the network for 'unauthorised' files. The ICT Team will ensure that an adequate firewall and internet content filtering are employed to restrict external access and activity to the Trust / School ICT network and to protect the internet connection.

The ACET Network Manager and Senior ICT Technicians will always ensure that an adequate email and filtering security software is in place to protect the Trust systems from obvious threats, however there is also a degree of personal responsibility to use the systems safely, vigilantly and appropriately.

4.3.4 Data protection

All data within this policy will be processed in line with the requirements and protections set out in the General Data Protection Regulation (GDPR) and the UK-GDPR post-Brexit transition. Please see Appendix 2 for more details of the legislation governing the Trusts Data Protection approach

4.3.5 Other considerations

The ICT Team must be made aware of any perceived threat, suspicious activity, or phishing attack. This should be via the usual channels but should be flagged as a security concern to ensure appropriate escalation.

The following behaviours are strongly encouraged:

- Report to ICT the presence of any discovered, unexpected, or unexplainable ICT hardware
- Report to ICT any perception of a weakness in the Trust's ICT security
- Avoidance of non-work-related web activity on Trust networks, even during breaks

The ICT Team will always respond to security threats, information or risks urgently, with a pre-defined escalation route being observed. In addition, the ICT Team should provide regular training, and promote good security practice and highlight new threats through the use of briefing notes.

5. Limitations of this Policy

While every endeavour is made to secure the ICT systems, the nature of exploits and malicious actors is such that it is possible a route may be found to breach the security of the systems. In this case, and ICT Cyber Response Plan is enacted.

6. Policy Breaches

By using Trust computer equipment, networks, software or systems detailed in this policy you are accepting the terms and conditions it sets out. All staff and pupils / students of Aston Community Education Trust are expected to adhere to the sections in this policy where it is appropriate to them. Serious or repeated breaches of this policy may result in disciplinary action the severity of which will be determined by the Chief Executive Officer (CEO) and / or Academy Trust Directors.

7. Social Media

Please see the ACET Social Media policy for specific guidance and advice on the safe use of social media.

8. Using your own equipment (BYOD – Bring Your Own Device)

A number of Trust academies currently deploy a Visitor/BYOD network that is totally segregated from the main academy network and allows staff and pupils/students to use their own devices to connect to online services independently of the academy network. This type of network offers great flexibility for working but also brings security implications and support issues. This section defines the type of devices that can be used, how you can use the network facility, what the security implications are and what constitutes a breach of the BYOD policy.

By being segregated, this network does not allow access to the main academy network, any files – personal or shared, nor any applications or devices. You can still access your own documents and email.

By its very description, BYOD means that the device you use to connect to the academy's networks and systems is your own personal device. As such, and with the exception of helping you connect your device, **we cannot offer any technical support for any aspect of your device, its success or failure to perform a particular function, nor its suitability for accessing the BYOD network**. In addition, security of your device, its content and availability for use cannot be guaranteed to be error free or totally secure from being accessed by other devices. By using the BYOD network with your own devices you accept and acknowledge that at no point will the academy or Trust be liable for any errors, omissions, technical deficiencies, security breaches, loss of data or other technical issue.

Use of your own personal equipment via the Trust and academy BYOD network(s) is entirely at your own risk.

Appendix 1: Acceptable Use Policies / Codes of Conduct

These policies are aimed at staff, pupils / students and some third-party users of the Trust ICT Systems. They are general rules that, in conjunction with this and other policies, define your responsibility when using the Trust ICT Computers and handling data. Staff and pupils / students are required to accept the Terms and Conditions set out in these policies and are reminded of this during the log on process to any Trust or academy computer. By logging onto a Trust or academy computer, they indicate their acceptance of these policies and agree to abide by the terms and condition they set out.

Each policy will be distributed to staff and pupils / students on starting with their academy, updated and re-distributed according to the timeframes set agreed by the Trustees and academy Governing Bodies.

These pages can be printed and distributed for each student / member of staff at the commencement of them starting with the academy / Trust or after every review of this policy. Please see section 13 of this policy for information about the renewal process of this document and any associated text.

1.1 AUP Students – Secondary

ICT and Computer Acceptable Use Agreement: Pupils - Secondary

I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.

- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved and attended by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system or any other computer security system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / carer may be contacted.

1.2 AUP Pupils – Primary

Primary Pupil Acceptable Use

Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately use the Internet to search for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

1.3 AUP Staff, Governors and Temporary Users

Staff, Governor and Temporary Users
ICT Equipment Acceptable Use Agreement & Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This Code of Conduct supplements the E-Safety and Data Security Policy covering the use and procedures associated with all aspect of the Trust IT Computer Network. By using the ICT Equipment within the Trust academies, you agree to be bound by the terms and conditions of this document, a summary of which is detailed below:

- I will only use the school's email / Internet / Intranet / VLE / VPN and any related technologies for professional purposes or during specific time, when it acceptable for personal use.
- I will comply with the E-Safety Policy and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Chief Executive Officer (CEO) or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the IT Technical Support Department.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff, Chief Executive Officer (CEO) or Governing Body.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Chief Executive Officer (CEO). I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand this forms part of the terms and conditions set out in my contract of employment and by using the school ICT Equipment I agree to be bound by this code of conduct and the Trust E-Safety and Data Protection Policies.

Appendix 2: Legal Issues and Further Guidance

There is a large range of legislation that covers the use of information, ICT equipment, software and the storage and processing of data. Listed below are some of the relevant documents and acts that contain references to the use of ICT:

- The UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Privacy and Electronic Communications Regulations UK
- Freedom of Information Act 2000 (there are UK outstanding changes to this legislation)
- ICO Employment Practices Code (not updated for UK GDPR)
- The Copyright and Related Rights Regulations 2003
- Libel Act 1843 (Defamation act 2013)
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994 (there are outstanding changes to this legislation)
- Malicious Communications Act 1998
- Communications Act 2003(there are outstanding changes to this legislation)
- Teachers Standards (parts 1 and 2) – 2011 (updated 2013)
- Electricity at Work Regulations 1999
- The Waste Electrical and Electronic Equipment Regulations 2013

All of these documents are relevant to this policy (in whole or in part) and where possible the document states which legislation is relevant to a particular section. Where a policy is awaiting changes, any up to date information can be obtained by searching for the relevant legislation on the Government website:

https://www.legislation.gov.uk

GDPR

The General Data Protection Regulation (GDPR) 2018 is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR replaced the data protection directive of 1998 and became enforceable from 25 May 2018. Unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

A full guide the General Data Protection Regulations is available from the gov.uk website:

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

GDPR and Brexit

The Brexit transition period ended on 31st December 2020. The UK's Data Protect Act 2018 has already enacted the EU GDPR's requirements into UK law, and with effect from 1 January 2021, the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a new, UK specific data protection regime that works in a UK context after Brexit as part of the DPA 2018.

This new regime is known as 'the UK GDPR'.

This document covers the acceptable use of Trust IT equipment as well as the electronic use of data and the devices that are used to store, retrieve, distribute and manipulate data as it relates to the ACET privacy notices.

The ACET GDPR policy is a comprehensive document intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. The full document plus the ACET Privacy notices for Staff and pupils / students can be downloaded from the ACET website: www.astoncetrust.org

9. Acceptance

You are reminded that by logging into and using the ICT Network Facility or Trust / Academy computers you agree to be bound by the terms and conditions that this document sets out. You are further reminded of this statement each time you boot any computer connected to the trust or academy networks.

Please make sure you read and understand this document in full before you log into any of the Trust or Academy computers.