ICT Acceptable Use Policy

Archway Learning Trust

Approved: June 2020

Responsible Officer: Operations Director

Trust Ethos, Mission, Vision and Values

The Trust believes in the transformational power of education for each individual and that this is enhanced through collaborative working between the academies.

Working together, transforming lives

Contents

Where the word 'Trust' is used in this document it refers to Archway Learning Trust.

Where appropriate the Academy Advisory Boards (AABs) of individual academies will publish details of the procedures and practices to implement Trust policies.

The term 'Trust Executive Leadership Team' (ELT) is comprised of the Chief Executive Officer, Director of Education, Executive Principal, Chief Operations Officer, each Academy Principal or Head Teacher.

Where the word 'users' or 'employees' is used it refers to staff, future staff issued with ICT access and/or hardware, trustees, AAB members, volunteers and regular visitors.

Where the phrase 'Senior Leader' is used, this refers to the ELT, Principals, Heads of School or Business Services Director within the Trust.

Related Policies and Procedures:

- Bullying and Harassment Policy
- Code of Conduct
- Data Protection and Freedom of Information Policy
- Disciplinary Policy
- Finance Policy
- Safeguarding Policy
- Social Media Policy
- Whistleblowing Policy
- Teacher Standards
- Procedure for Dealing with Allegations of Abuse Against Staff and Volunteers
- Social Media Guidance for Personal Use

1. Policy Statement

1.1. Archway Learning Trust recognises that technology is an integral aspect of the lives of employees, students and stakeholders. These technologies can facilitate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for more creative and productive learning.

1.2. The Trust is committed to maximising the opportunities which technology provides for all individuals to learn, engage, communicate, and develop skills within a safe and professional culture which complies with confidentiality and data protection requirements.

1.3. The Trust will provide employees, future employees where appropriate, AAB members, volunteers and regular visitors **("users")** with access to Information Communications Technology (ICT) to enhance their work and the learning opportunities for students, where appropriate.

1.4. An authorised user has the privilege and benefit of accessing Trust facilities for personal use in a manner which is consistent with their contract of employment and in accordance with the Trust's Code of Conduct.

2. Scope and Principles

2.1. It is important that users acknowledge the role they play in upholding the reputation of the Trust in both their professional and private lives. Individuals must ensure that their personal use of ICT and technology, including social and gaming media, does not bring the organisation into disrepute and/or damage public confidence in the Trust's ability to provide a safe and appropriate environment for students and colleagues.

2.2. All Archway Learning Trust users must comply with this policy and take appropriate measures to ensure that they use ICT in a safe and responsible manner, both inside and outside the work place. This includes the wider use of technology, including but not limited to, mobile devices and applications, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.

2.3. Inappropriate use of ICT by an employee may be treated as misconduct under the Trust's Disciplinary Policy and in some cases it may amount to gross misconduct. Inappropriate use of ICT by a AAB member or volunteer could result in their removal from office or volunteer arrangements being considered by the Board of Trustees.

2.4. Users are expected to comply with the spirit of this policy which is intended to clarify the Trust's expectations of users in relation to the use of ICT in order to ensure:

- that users understand how to use ICT, including the internet and other communications technologies, for educational, personal and recreational use in a responsible and appropriate manner;
- that Trust ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and/or users at risk;
- that users are protected from potential risk in their use of ICT in their everyday work and practice;

- that appropriate professional boundaries are maintained in order to protect students, staff, trustees, AAB members and volunteers from potential misinterpretation and/or abuse of the relationship between those parties.

2.5. All users will be asked to sign receipt of this policy at commencement of employment as confirmation that they have read and understood the content and agree to use ICT in accordance with these expectations. Electronic versions of the policy will be issued to users via their IT login home screens on a termly basis and they will be required to confirm that they have read and understood the content electronically.

2.6. Questions about this policy and requests for training or information in relation to appropriate use of ICT should be directed to the IT Services Team as appropriate. Users may also wish to contact their trade union representative for advice and guidance as appropriate.

2.7. This policy does not form part of any employee's contract of employment and it may be amended at any time following consultation with staff and recognised trade unions.

3. ICT Systems and Equipment

3.1. Archway Learning Trust ICT facilities, equipment and services are provided to authorised users for the purposes of Trust business, albeit the Trust recognises that users may occasionally use the ICT equipment for personal use (please see paragraph 1.4).

3.2. In using technology and services that the Trust provides, users must adhere to following accepted uses:

3.2.1. Hardware

- ICT hardware is provided to enhance and improve educational outcomes and should be used to undertake Trust business. The access to and use of desktops, laptops, tablets and mobile devices must be backed with a clear business case and line manager approval before being provided.

- The Trust's IT Service manages the issuing of hardware to staff. Users are not permitted to obtain IT hardware using Trust funds without approval from IT Services.

- Users are expected to take reasonable care in the use of ICT hardware and must report damages or faults at the earliest opportunity. Where issues occur due to the negligence or deliberate misuse of hardware this cost will be passed onto the individual or parties involved. Where users are provided with mobiles devices, they are required to take reasonable care of the equipment both inside and outside of the Trust at all times to avoid loss or damage to it.

3.2.2. Software

- The core aim of software provided for use by users is to deliver education experiences to our young people and undertake Trust business that supports this core aim.

- It is not permitted that Trust provided software is used for personal gain nor are users permitted to use software for purposes which conflict with the Trust's core aims.

- The definition of Software is broad and includes all applications installed on Laptops, Tablets, Desktops and Servers, as well as all online services such as Office365 and online platforms.

- All software installed on Trust systems must be licensed and this recorded with IT Services.

- Software must be approved for use; and therefore this must be sought from the IT Services before purchasing, installing or using any software on the Trust's systems. Any online system with Trust data being stored in it must be bought to the attention of the Data Controller and IT Services for risk assessing and approving ensuring GDPR compliance. The storage of software programmes that are unlicensed is prohibited.

- The Trust will put preventative measures in place to ensure staff do not inadvertently change system settings. Users are prohibited from adversely changing system settings beyond those that are delegated to them. Although users may need to make minor tweaks to PC settings, such as icon layouts, these changes must only be made to equipment the user is working on. This provision does not apply to System Administrators who are required to make system-wide changes as part of their role.

- Users are not permitted to access software, systems or files outside of their role unless specific approval is provided by a Senior Leader.

- Where there are concerns that software is not being used safely, outside of a user's role or not for the purpose intended these should be reported to a Senior Leader at the earliest opportunity.

- Where there are concerns that a user becomes aware of having access to data outside of their delegated limit this should be reported to IT Services without delay.

3.2.3. **Internet and Network Bandwidth**

- The Trust provides a comprehensive organisation-wide connected network for the benefit of all users, which includes each site and remote working. The network is designed to be robust and resilient with ample capacity to access network resources and the internet from wherever a user is accessing our network.

- Unless specifically authorised, users should not be using the Trust's networks to access or upload unreasonably large files; this includes files from or to the internet or internal network location.

- Internet usage is monitored and the use of the Trust's internet connections should primarily be used for Trust business and their use in line with the behaviour standards set out in this policy.

3.2.4. **Monitoring and Filtering**

- All IT systems across the Trust are actively monitored for the protection and safety of the Trust and all users and in order to ensure compliance of this policy and any legislative duties. The Trust reserves the right to access all material stored on the Trust ICT systems, including that held on the personal areas of user accounts, including email mailboxes, for this purpose.

- Monitoring takes place in relation to all IT systems across the Trust and includes all mobile devices, software, systems and emails. Monitoring applies to these systems all of the time and extends to devices provided to users for use outside of the Trust network; including use of mobile devices outside of the Trust premises, both during and outside of normal working hours. Monitoring processes may not be able to distinguish

between business and personal files or messages and so all items stored on any media are deemed to be business communications. If an employee chooses to make use of Trust facilities for personal files or correspondence, they must be aware that their files and emails will not be private.

- Monitoring actively looks for violations of the accepted uses of Trust systems, this includes but is not limited to: keyword matching, image monitoring and application usage. The accepted usage of systems is defined in this policy and monitoring will seek to identify activity that does not conform to the standards of behaviours and conduct expected by the Trust.

- Monitoring is centralised by the Trust and access to the monitoring software is limited to specific personnel where access is required as part of their role.

- Where users are concerned that this policy has been infringed they should make every effort to report this to a Senior Leader at the earliest opportunity.

3.2.5. **Communications**

- Users should ensure that they maintain professional standards when using any systems and conduct themselves in a manner which is appropriate to the audience and of suitable content. Users should ensure that they avoid the use of aggressive or inappropriate language during such communications at all times.

- Users should also understand that others may have different opinions and should respect these opinions when communicating with each other.

- Occurrences of spoof email addresses and malware infections attempts are ever increasing and staff should be ever vigilant when using email systems. Treat unsolicited e-mails with caution. Users should not open any e-mail attachments from an unknown or suspicious sender, without first considering whether it is from a trusted source and was expected. If in any doubt, do not open the email and forward it to IT Services for further advice. Please also contact IT Services if unwanted, unsolicited e-mails continue to be received.

- The threat of SPAM emails is constantly evolving and the Trust will make every effort to reduce the volume that users receive into their inbox. Staff should follow guidance issued by the IT Services when they receive SPAM.

3.2.6. **Usernames and Passwords**

- Users will be provided with a unique username and password when granted access to IT systems at the Trust. This password is temporary and must be changed at first login and meet system complexity requirements.

- Users must not disclose their username or password to any other user or third party. It is acceptable for a user to disclose their username to IT Services when receiving support.

- Passwords must be changed by users once every term and must meet the criteria as issued by IT Services for all password controlled systems.

- Users are not permitted to allow anyone else to use their account unsupervised. Under no circumstances should students or guests be logged into Trust systems with an account belonging to a member of staff unless they are supervised at all times.

3.2.7. **Service Reporting**

- Users should report issues, problems and faults through the Trust's Service Desk Software. Users can also use the Trust's Service Desk email: servicedesk@bluecoat.uk.com

- Users should make every effort to provide as much information as possible, including device name, location and a description of the issue with any error messages.

3.2.8. **Encryption and Removable Media**

- The Trust understands that mobility plays a key role in facilitating the most effective use of ICT for users. Mobility of users inherently introduces more risk to the Trust, especially in relation to the loss of sensitive data.

- The Trust will encrypt all mobile laptop and tablet devices provided by the Trust to users and users are prohibited from disabling this setting. Memory sticks provided by the Trust cannot be backed up and users must ensure data is adequately saved on Trust systems.

- Personal memory sticks are prohibited from being used and users are expected to request a Trust encrypted memory stick from the IT services or use more secure methods of transferring/saving work such as Trust operated email and cloud based systems.

- Users must use Trust-owned memory sticks which have been encrypted and issued by IT Services.

- Users may use CDs or DVDs to access or burn files required to undertake their roles, though must allow the system to complete virus checking automatically before being used.

- The Trust reserves the right to remotely disable or wipe data from devices that are reported lost or stolen.

- Where users wish to load data onto the system, this should be facilitated by IT Services and users are directed to report the request as laid out in this policy.

3.2.9. **Backup and Virus Protection**

- The Trust will take all reasonable steps to provide anti-virus and malware and anti-spyware protection to all devices owned by the Trust.

- Users are not permitted to add personal devices to the Trust network without the express permission of IT Services.

- Users are not permitted to disable any Anti-Virus or security protection system employed by the Trust.

- The Trust will comply with all legal and exam board requirements as well as follow best practice in backing up its IT systems. The Trust will also undertake regular disaster recovery scenarios for the purpose of testing its Disaster Recovery Plan.

3.2.10. **Mobile Phones**

- Users who have been given a Trust mobile phone will be expected to sign for its use upon receipt, and return it to their IT Business Partner when no longer required or when a user leaves/changes their post at Archway Learning Trust.

- Staff are responsible for the safekeeping of the mobile phone. Any defects/loss of mobiles must be reported immediately to the IT Service Desk. Where it is deemed damage or loss is due to wilful negligence, the user will be responsible for replacing the device.

- Calls from Trust mobile phones are permitted for business use only.

- Personal mobile phones, devices or cameras should not be used to photograph students. Any photography must be taken using Trust equipment and in accordance with the Trust's Data Protection and Freedom of Information Policy and practices to ensure the necessary parental consent has been given in relation to the use of images.

- Any photography or images taken of students or colleagues should be downloaded to the Trust network as soon as it is possible. Please seek assistance from IT services. All images on the mobile device should be removed.

3.2.11. **Mobile Working**

- Trust mobile devices have the ability for users to work remotely when away from Trust premises. Users are expected to use their equipment to the same standards expected as if they were present within the Trust academies.

- Users should be extremely mindful of the network connection they use to connect to Trust services with their device. Users are advised against connecting to "Open" networks to prevent unauthorised capture of data transferred between the Trust and the device.

- Users should use Remote Access or VPN wherever possible to work remotely. Where this is not possible, users can work locally on their device; however must ensure documents and work is saved in their S Drive for syncing with the Trust on return.

- Users are prohibited from leaving any mobile device, when working remotely, unattended whilst unlocked. Devices that need to be unattended should be at least locked, or fully shut down to prevent any unauthorised access attempt.

- The Trust will enforce an inactivity timeout of mobile devices of 30 minutes.

4. Standards of Behaviour and Conduct

4.1. Individuals who work with children and young people are subject to a greater level of public scrutiny in relation to all aspects of their conduct due to the nature of their work. It is important that all users adopt the same high standards of behaviour and conduct when using ICT technology as those standards expected in all other forms of interactions with

students, colleagues and stakeholders (please refer to the Code of Conduct for further details).

4.2. Users should ensure that their use of ICT and technology is consistent with their professional responsibilities and that the language they use via electronic means is appropriate to the audience and of suitable content, regardless of the location that they are using the ICT systems. They must not use Trust ICT systems, equipment or devices to attempt to upload, download, access or store any materials which are illegal or deemed to be otherwise inappropriate by the Trust. This includes, but is not limited to material which:

- is obscene, illegal, pornographic or paedophilic;
- is defamatory, libellous, deceptive or unfairly criticises or misrepresents any individual or organisation;
- violates the privacy of others;
- may be considered to be promoting violence or terrorism in any way;
- is discriminatory;
- is abusive or may be considered as harassment or bullying;
- is generally distasteful or could reasonably cause harm, offence, annoyance, inconvenience, anxiety or upset to others.

4.3. This requirement also extends to the use of personal ICT equipment or devices whilst on Trust premises or whilst acting in the capacity of a representative of the Trust.

4.4. In using ICT and technology, users should adopt the following practices:

4.4.1. **Use good judgment**

- exercise sound, professional judgment throughout all use of ICT and technology;
- familiarise themselves with the Trust's Code of Conduct and Social Media Policy and ensure that their use of ICT and technology complies with the expectations set out in the policy;
- regardless of any privacy settings, assume that all of the information they share through electronic communications and social media forums are potentially public information.

4.4.2. **Treat others with respect**

- ensure the use of the internet, network resources, electronic communications and online sites is always conducted in a courteous and respectful manner and in a way that is appropriate to the audience;
- recognise that language and tone used via electronic communications can be misunderstood more readily than face to face or telephone discussions, ensuring electronic communications are conducted carefully with this in mind and in a professional manner.

4.4.3. **Use ICT and technology responsibly and ethically**

- unless specifically authorised to speak on behalf of the Trust/Academy as a spokesperson, ensure the views expressed through ICT and technology are identified as employees own;

- ensure the use of ICT and technology is used to deal with school-related matters that are within the remit of the staff member, AAB member or volunteer;

- be open about an employees' affiliation with the Trust and the role/position the employee holds;

- use trusted sources when conducting research via the internet, recognising that some online content is unverified, incorrect or inappropriate.

4.5. Cyber bullying or cyber harassment are forms of bullying or harassment conducted using electronic means of communication which can be invasive of privacy at all times. Such acts may also constitute criminal offences and will not be tolerated under any circumstances. Please refer to the Trust's Bullying and Harassment Policy for further details.

5. Confidentiality

5.1. It is the responsibility of individual users to ensure the security of any personal, sensitive, confidential and classified information which is accessed or dissimilated through Trust ICT systems.

5.2. Users should not publish, post or release information that is considered confidential. They should not reveal information pertaining to their work with the Trust on any social networking site or public forum.

5.3. Users must ensure that their workstations are not left unattended whilst logged on to the Trust's ICT systems without locking their access and should ensure that their passwords are held securely. Users should apply the same security measures when accessing Trust ICT systems remotely, such as from home.

6. Reporting Concerns

6.1. All users have a duty to report any incidents of use of the ICT systems which do not comply with this policy to their line manager. If their concern relates to the use of ICT systems by their line manager, they should raise the matter with an appropriate Senior Leader.

6.2. In situations in which mistakes occur using ICT and/or technology, the user should take appropriate corrective action at the earliest opportunity, including liaising with any affected individuals. In circumstances involving significant errors, or those which may constitute a breach of data protection legislation or responsibilities, such as mistakenly divulging confidential information, users should alert the relevant Senior Leader immediately.

ICT Acceptable Use Policy Acknowledgement

My signature acknowledges that I have read, understood and will adhere to the Archway Learning Trust ICT Acceptable Use Policy. I also acknowledge that I will report any breaches or concerns relating to compliance of this policy immediately to my line manager and a Senior Leader, Principal, Executive Principal, CEO or Chair of the Academy Advisory Board or Chair of the Board of Trustees, as appropriate.

_____

Signature:	
Printed Name:	
Job Title/Capacity:	
Date:	