Altrincham CE
Aided Primary School

Altrincham CE Primary School Primary School

Staff & Governor Acceptable Use Policy (AUP)

2025-26

Our Vision:

At Altrincham CE Primary, we are rooted in the love of Christ, nurturing each pupil's unique gifts and potential.

Together, we grow strong in faith and character, bearing fruit in our community as we learn, support one another, and blossom into the best version of ourselves.

Our Values:

Policy information and Review

Named individuals with designated responsibility

Academic Year	Designated Lead Person(s)
2025-26	Sam Halliwell, Sam Thompson, Sue Watkins

Policy creation date & duration

Creation date	Changes made to previous policy	By whom	Review date
January 2026	Updates based on KCSiE 2025	Sam Thompson	September 2027

Ratification by Governing Body

Academic year	Date of ratification	Chair of Committee	Chair of Governors
2025-26	11.02.26 - C&S	Colette Coverley	James Chillman

Acceptable Use Policy and Agreement

This policy is designed to prescribe acceptable use of school technology for staff and governors.

ACE provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of ACE's ICT systems and infrastructure
- Define and identify unacceptable use of ACE's ICT systems and external systems
- Educate users about their data security responsibilities
- Describe why filtering and monitoring of the ICT systems may take place
- Define and identify unacceptable use of social networking sites and school devices
- Specify the consequences of non-compliance

This policy applies to staff members, governors and all users of ACE's ICT systems, who are all expected to read, understand and abide by the aims of this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by ACE of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner.

If you are in doubt and require clarification on any part of this document, please speak to the Executive Head Teacher.

Provision of ICT Systems

All equipment that constitutes ACE's ICT systems is the sole property of ACE.

No personal equipment should be connected to or used with ACE's ICT systems. Users must not try to install any software on the ICT systems without permission from the Executive Head

Teacher. If software is installed without permission, it may cause damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Executive Head Teacher is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Network Access and Security

Users are not permitted to make any physical alteration either internally or externally, to ACE's computer and network hardware.

All users of the ICT systems at ACE must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the phase or department for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Executive Head Teacher as soon as possible.

Users should only access areas of ACEs computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of ACE ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on ACE ICT systems or cause difficulties for any other users.

School Email

Under no circumstances should a pupil be allowed to use a staff computer or device, unless being directly supervised by the account owner.

Where a staff member is provided with a school email address, it is for academic and professional use with reasonable/no personal use being permitted. ACE's email system can be accessed from both ACE computers and via the internet from any computer. All school-related communication must be via ACE email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are strictly prohibited
- Sending of attachments which contain copyright material to which ACE does not have distribution rights is not permitted
- The use of personal email addresses by staff for any official school business is not permitted
- The forwarding of any chain messages/emails etc. is not permitted
- Spam or junk mail will be blocked and reported to the email provider
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
  - Email encryption
  - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent)
  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line nor in the main body of the text either. Initials should be used.

- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be formally recorded using CPOMs Staffsafe
- Staff are encouraged to develop an appropriate work life balance and emails should not be sent before 7.45am, after 6pm, at weekends and during school holidays
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be
- School email addresses and other official contact details must not be used for setting up personal social media accounts
- Emails must not contain personal opinions about other individuals e.g., other staff members, children or parents

Internet Access & Filtering/Monitoring[1]

Internet access is provided for academic and professional use.

ACE's internet connection is filtered, meaning that inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to the Executive Head Teacher.

Staff and governors must not access from ACE's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials

[1] Filtering and monitoring have distinct differences:
Filtering selectively blocks or allows content based on predefined criteria, often used to restrict access to inappropriate or harmful material.
Monitoring involves continuous observation and recording of activities or data, aiming to identify patterns, behaviors, or potential issues.

- transmitting a false and/or defamatory statement about any person or organisation
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others
- transmitting confidential information about ACE and any of its staff, students or associated third parties
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for ACE)
- downloading or disseminating material in breach of copyright
- engaging in online chat rooms, instant messaging, social networking sites and online gambling
- forwarding electronic chain letters and other materials
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, ACE may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital Photography

ACE encourages the use of iPad photography and videos to record curriculum learning and co-curricular activities. However, staff should be aware of the following guidelines:

- If a child's parents have indicated that they do not give photo/video consent, then photos of their child should never be taken

- Photos for the website, social media, newsletters or press must only include the child's first name, if named at all
- The use of personal digital cameras in school is absolutely forbidden, including those which are integrated into mobile phones, iPads or similar
- Staff must not, for any reason, take photos of children using their own devices
- All photos taken using school technology should be downloaded to ACE network as soon as possible.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

Removable Media

Staff and governors should not store school content on USB sticks (or similar). All school material should be stored on the shared drive.

Mobile Phones

Mobile phones are permitted in school with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children.
- Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker
- Personal mobile phone cameras are not to be used on school trips except in an emergency
- All phone contact with parents regarding school issues will be through ACE's phones.
- Personal mobile numbers or any other personal details should never be shared with parents

Use of Whats App & Social Media

WhatsApp is not permitted for use on School issued devices or personal devices for School business.

The school has no jurisdiction over staff using WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members regarding school business using their personal WhatsApp accounts.

School business must be conducted using ACE-issued email accounts.

With regard to Social Media, the key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of ACE, staff and families at all times and must treat colleagues, parents, children and associates of ACE with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or ACE's reputation, nor the reputation of individuals within ACE are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Executive Head Teacher.
- Members of staff will notify the Executive Head Teacher if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in ACE/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites apart from by prior agreement with the Executive Head Teacher, using ACE accounts.
- No details or opinions relating to any pupil or family are to be published on any online forum.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others via social networking sites.
- No opinions regarding another member of staff are to be posted.
- No photos or videos which show pupils of ACE who are not directly related to the person posting them, should be uploaded to any site other than ACE's website.

- No comment, images or other material may be posted anywhere, by any method that may bring ACE or the profession into disrepute.
- Users must not give children or parents access to their area on a social networking site. Staff members who are also parents should speak to the Executive Head teacher regarding what is acceptable and what is not.

ACE receives weekly emails regarding filtering and monitoring, and via its ICT support team will periodically exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of ACE's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided
- maintain the systems
- prevent a breach of the law, this policy or any other school policy
- investigate a suspected breach of the law, this policy or any other school policy

Monitoring of the ICT Systems

Any unauthorised use of ACE's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Executive Head Teacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

ACE reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Failure to Comply with Policy

Any failure to comply with the policy may result in disciplinary action.

Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.