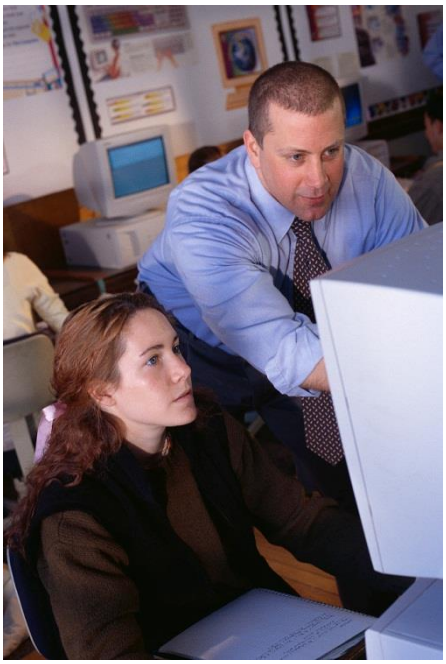
Action Community Enterprises CIC (ACE)

Acceptable Use of ICT Policy



Policy number:	
Version:	1.0
Policy holder:	Lou Gardiner
Approval board:	ACE Board of Directors
Date of original approval:	September 2022
Date of latest approval:	September 2024
Review period:	Annually
Date of next review:	September 2025

Purpose

The purpose of this policy is to ensure that employees, workers, and other people accessing ACE's Information Communication Technology (ICT) understand the ways in which the ICT equipment and Wi-Fi is to be used.

The policy aims to ensure that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk. Where reference is made to ACE's ICT, this also includes any specific facilities, equipment, and networks. Any reference to ACE includes all sites.

Employees are provided with free access to a wide range of ICT provision to enable and assist their work and support their development. By using the ACE's provision, or using personal devices on-site, which may require access to the ACE's Wi-Fi, all users are agreeing to adhere to this policy.

Users are responsible and personally accountable for their use and activity on the ACE's ICT systems and Wi-Fi. Any use that contravenes this policy may result in the ACE Disciplinary Policy and Procedure being invoked. In addition, ICT usage privileges may be withdrawn or reduced.

1. SCOPE

This policy applies to all employees, workers and others accessing ICT at ACE and they will be termed as 'users' within this policy. This policy details ACE's expectations of all users of ACE's electronic communication, including, but not limited to telephone, social media platforms, email, internet and ICT systems.

2. ROLES AND RESPONSIBILITIES

The ACE Board is responsible for approving this policy.

The CEO is responsible for ensuring that staff and managers are aware of and adhere to this policy and procedure and that breaches are managed swiftly, effectively, fairly and consistently.

The Managing Director and Leads are responsible for ensuring that all employees understand their responsibilities when using ICT at work and that systems are used and managed effectively. Anglian Internet will limit access to websites and may be directed to monitor usage and report any breaches to the CEO or Managing Director.

Managers must ensure they report any breaches of this policy immediately to the CEO. Data protection breaches must also be reported to the Data Protection Officer.

All users must ensure they understand and adhere to ACE's expectations regarding electronic usage and communications, seeking further clarification and advice where appropriate. If they require access to a website, which is blocked, they should raise the issue with their line manager.

3. EQUALITY AND DIVERSITY

ACE is committed to:

- Promoting equality and diversity in its policies, procedures and guidelines
- Ensuring staff are protected from unlawful direct or indirect discrimination resulting from a protected characteristic (e.g. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation)

4. KEY PRINCIPLES

This policy details the minimum expectations of ACE when users are accessing ACE ICT systems and Wi-Fi. Failure to comply with these requirements may be viewed as a breach of this policy and could be viewed as a disciplinary matter, with serious breaches potentially leading to dismissal.

- Passwords and login details must remain confidential.
- Users must not intentionally install software unless specifically authorised to do so.
- Users must not intentionally introduce viruses or other malicious software.
- User must lock ICT equipment when not in use.

ACE's e-communications systems must not be used to:

- Store, send or distribute messages or material which may be perceived by the recipient or ACE as:
    - Aggressive, threatening, abusive or obscene.
    - Sexually suggestive.
    - Defamatory.
    - Sexually explicit.
    - Discriminatory comments, remarks, or jokes.
    - Offensive.
- Act in a way that contravenes ACE's policies, legislative, statutory, or professional requirements.
- Bring the ACE into disrepute.
- Disclose sensitive information or personal data to unapproved people or organisations.

- Breach the ACE's Data Protection Policy, General Data Protection Regulations, or the Data Protection Act 2018.
- Intentionally access or download material containing sexual, discriminatory, offensive, or illegal material.
- Participate in online gambling, including lotteries.
- Participate in online auctions unless authorised to do so for work-related matters.
- Originate or participate in email chain letters or similar types of communication.
- Harass or bully another person.
- Create material with the intent to defraud.

If a user accidentally accesses inappropriate material on the internet or by email, they must immediately disconnect and inform their manager.

Users must not bring into ACE any material that would be considered inappropriate. This includes files stored on memory sticks, CD, DVD, or any other electronic storage medium, or accessing information via ACE's Wi-Fi, which would be viewed inappropriate. Under no circumstances should any users of ACE's ICT systems download, upload, or bring in material that is unsuitable for children or schools. This includes any material of a violent, racist, or inappropriate sexual nature. The transmission, display, storage, or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution. If in any doubt, staff should check with their line manager. Staff are also encouraged to refer to the film classification system as a guide.

Users must not use ACE ICT systems or Wi-Fi for the creation, transmission or access of pornographic, illegal or gambling content.

Occasional appropriate and reasonable personal use of ICT equipment and or Wi-Fi on-site is permitted provided such use of the ACE systems:

- Is restricted to the user's own time.
- Doesn't interfere with the performance of duties.
- Doesn't adversely impact on the performance of ACE's ICT systems or the network.
- Doesn't contravene the requirements of ACE's Code of Conduct, or other ACE policies.
- Doesn't include material of a pornographic, illegal, or gambling nature.

Users must always be mindful that they are responsible and personally accountable for their use of ACE ICT systems and networks. All internet-based activity on personal devices is monitored and logged whilst using the Wi-Fi. Misuse of ACE ICT systems and networks belonging to or associated with ACE may breach other policies and/or procedures and/or the law. Users can be held personally liable and such breaches may lead to civil, criminal, or disciplinary action including dismissal.

Users are responsible for all files that are stored in their storage area and any visits to websites by their user account. Users must not breach the copyright of any materials whilst using ACE's ICT systems. This includes, but is not exclusive to:

- Copying, or attempting to copy, any of ACE's software.
- Storing any files in their personal storage area which require copyright permission, and where that permission is not held.

Any breach of copyright whilst using ACE's ICT systems is the individual user's responsibility and ACE cannot accept any liability or litigation for such a breach.

Users must ensure that:

- They keep personal data safe, taking steps to minimise the risk of loss or misuse of data.
- Personally identifiable and sensitive, confidential data is protected with the use of passwords, locking of computers, logging off shared devices, use of encryptions where appropriate and increasing the use of remote access rather than transporting or transferring information.
- Personally identifiable, sensitive and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, surfaces or laptops, and CDs or DVDs) and it must not be stored on users' personal devices (e.g. home PCs, mobile 'phones).
- When using mobile devices (e.g. surfaces and laptops) users encrypt/password protect documents; password protect the device; ensure the device has appropriate virus and malware checking software
- Data is only retained, destroyed and deleted safely in line with the ACE's Data Protection Policy and associated procedures and guidelines.

Users are encouraged to use remote access, OneDrive, where possible rather than unencrypted portable devices.

Users must not save sensitive data on any form of unencrypted portable devices. Users must not download copy or attempt to install any software onto ACE computers/devices without checking first with their line manager. Any attempt by a user to compromise the security or functionality of ACE networks and its ICT systems, either internally or externally, will be considered as "hacking". It should be noted that "hacking" is illegal under the Computer Misuse Act 1990 and is prosecutable under law. Users must not deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network. All machines connected to ACE's ICT networks, must have appropriate, fully functioning and up to date antivirus software protection. If unsure, staff should seek advice from their line manager.

Users must not discuss or post content that reflects ACE or its employees in an inappropriate or defamatory manner through any electronic communication methods. This includes posting to social networking sites.

Users must not carry out any of the following deliberate activities:

- corrupting or destroying other users' data.
- violating the privacy of other users.
- disrupting the work of others.
- denying service to other users (for example, by deliberate or reckless overloading the network).
- continuing to use an item of networking software or hardware after ACE has requested that use cease because it is causing disruption to the correct functioning of the school's ICT systems and/or networks.
- other misuse of ACE's ICT and networked resources, such as the introduction of viruses or other harmful software to ACE's ICT systems
- unauthorised monitoring of data or traffic on ACE's ICT network or systems without the express authorisation of the owner of the network or systems.

This policy still applies when users access any of ACE's systems off-site.

ACE wishes to encourage all users to use the internet, however it is provided for work purposes and any use of the internet for personal reasons must be carried out in the user's free time. ACE cannot be held responsible for any failed personal financial transaction that may happen whilst using ACE's ICT systems.

Any attempt to circumvent ACE's firewall and internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the internet filtering systems. Such activity will be subject to ACE's Disciplinary Procedure in addition to any disciplinary outcome or sanction; it could also result in the removal of access to ACE's ICT systems or internet access.

There is a wealth of information on the internet; however, due the open nature of the internet, some material is either illegal or unacceptable. Any user who thinks inappropriate or illegal material is being accessed must report it to their line manager.

Whether users are using on-site ACE equipment, ACE equipment off-site or their own device via the ACE network, users should:

- limit personal use of the internet to own time.
- take advice from line managers before downloading large files or sending large amounts of data via a web-link – to avoid adversely impacting on the performance of the systems these transactions can be scheduled for off-peak times.
- if users accidentally access inappropriate material including unexpected 'pop-ups' they must disconnect immediately and inform their line manager.

Users must be mindful that if they use ACE equipment off-site, they need to minimise the risk of inappropriate information presenting on their ACE equipment

whilst at work. For example, the acceptance of cookies can result in pop-ups, which may contain material, which is inappropriate for some environments.

Users must not:

- access or download material which is pornographic, illegal or of a gambling nature.
- use the internet for personal use during working time, even if minimised on the screen.
- use systems to participate in on-line gambling or on-line auctions.
- download music or video files unless for ACE purposes.
- use 'peer to peer' or other file sharing services except where authorised to do so.

5. EMAIL AND ELECTRONIC COMMUNICATION ACCEPTABLE USE

When using ACE equipment, networks, email and electronic communication, ACE expects all users act responsibly and strictly according to the following conditions.

- Email facilities are provided as a method of enhancing communication of work-related issues. All users are responsible for the content of the messages that they send.
- Users are reminded that electronic communication can be monitored and random checks may be made.
- Email is the equivalent of a written document and can be used as an evidential record. With this in mind, care and consideration should always be taken before sending an email (e.g. freedom of information requests and subject access requests).
- Where there is a concern that a user has misused the email system, action may be taken in line with ACE's Disciplinary Procedure.
- All electronic communication between staff and service users must be carried out through ACE's ICT systems.
- ACE has enforced 2-factor authentication when accessing ICT outside of ACE buildings for staff.

Staff are advised not to communicate with pupils via social network sites, texts or telephone calls, although there may be occasions where it is appropriate and necessary (e.g. where staff and pupils are members of external groups or family and friend networks). If staff are unsure, they should seek advice from their line manager in the first instance. Staff must not share personal contact details with service users (mobile telephone numbers, non-work email addresses, social networking sites etc.) unless there is a justifiable reason (e.g. family or friend networks or external groups) and any unintended breach must be reported to the user's line manager immediately.

Users who receive emails regarding viruses or security threats must delete the email and report to their line manager. Users can minimise the risk of inadvertently introducing viruses by permanently deleting without opening emails that look

suspicious. Staff are encouraged to contact their line manager for advice and concerns that a virus may have entered a ACE system should be reported immediately. Users are advised that strict mail filters are in place to prevent any unwanted threat, whilst these measures are never 100% accurate, if you believe a genuine email or link within an email has been blocked, please contact your line manager for advice.

Users should ensure:

- personal email and texts should only take place in their own time.
- ensure that their messages are relevant and appropriate to targeted recipients (e.g. not using 'blanket' or 'all-user' emails).
- try to answer emails quickly, politely, and professionally.
- beware of 'email rage'. Email is quick and easy to use and can encourage ill-considered and even offensive messages.
- include a subject heading in every email so that the person receiving it knows what it is about.
- inform management immediately if the user receives or sees any offensive or sexually explicit material, spam, or phishing communications on the intranet or in email messages at work.
- they do not allow email and electronic communication to replace face to face communication.

Users must not:

- use mobile phones, in classrooms in front of pupils, unless they have sought permission from their line manager to do so.
- use a password in a way that can be seen by pupils.
- use email to circulate material, which is illegal, pornographic or of a gambling nature.
- use email as a substitute for good verbal communication.
- expect to receive a response to emails outside of normal working hours.

If staff are in doubt, they should seek advice from their line manager.

6. MONITORING

Authorised staff at ACE and its ICT providers may at any time monitor the use of ACE ICT systems and networks. The use of all ACE ICT systems and networks, particularly email and the internet, is subject to recording in order to detect and deal with abuse of the systems and fault detection. ACE will not, without reasonable cause, examine any private material that is discovered.

Personal data should not be stored on the network and users should not expect 'privacy' in relation to accessing websites, personal email correspondence, personal documents stored on ACE ICT equipment or networks or messages sent via the internet, as these, in principle, are subject to the same checking procedures applied to business related access and email correspondence.

7. PASSWORDS

ACE is responsible for ensuring data and the network is as safe and secure as possible. A weak password may result in the compromise or loss of data. As such, all users are responsible for taking the appropriate steps, as outlined below, to create and secure their passwords.

The aim of passwords is to protect user's data, children's welfare where access to confidential and sensitive data is allowed and to minimise the risk of unauthorised access to ACE networks. ACE enforces that users change their password each month, and enforces that:

- Passwords will be a minimum of fourteen characters.
- Passwords should not contain the user's account name or parts of the user's full name that exceed two consecutive characters. They should contain characters from three of the following four categories:
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

8. SECURITY

ACE staff must always remain vigilant in order to safeguard information and data and to protect the security and integrity of all ICT systems. Users of ACE computers and devices must ensure that:

- Computers/devices are not given to any unauthorised persons for safe keeping.
- Computers/devices are not left discarded or unattended in public places.
- All portable mobile computing devices and other IT equipment should not be left unattended in any vehicle at any time.
- Computers/devices must be adequately protected from physical damage.
- Computers/devices are not hired, lent or given out without authorisation from your line manager.
- All Computers/devices which are no longer required or which have reached the end of useful life must be returned via the line manager to be disposed of.

9. MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY

Effectiveness and compliance of this policy will be regularly monitored by ACE's Board.

10. REVIEW

This Policy and Procedure will be reviewed annually.

Appendix 1 SOCIAL MEDIA AND ACCEPTABLE USE GUIDANCE

Introduction

It is recognised that staff may be required to use social media for their work, and this guidance includes activities undertaken for work and personal purposes. This guidance applies to all social networking sites, chat rooms, forums, podcasts, blogs, texting, online encyclopaedias with open access (such as Wikipedia) and content sharing sites such as YouTube. Social media can serve as a learning tool where training videos and other materials are made easily accessible to learners in a user-friendly and engaging way. They can also be a useful tool for ACE to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can leave people vulnerable if they fail to observe a few simple precautions. Social networking websites provide an opportunity for people to communicate 'en masse' and share ideas regardless of geographical distance, however, there is the risk that posts and messages may feel private, when in fact they are in the public domain.

This guidance is applicable to all staff, trainees, external contractors, agency workers, volunteers and other individuals who work for, or may provide services on behalf of ACE, and references to staff in this guidance refer to all of the above people.

Safeguarding

As detailed within this policy, staff are advised not to communicate with pupils via social network sites, texts or telephone calls, although there may be occasions where it is appropriate and necessary (e.g. where staff and pupils are members of external groups or family and friend networks). If staff are unsure, they should seek advice from their line manager in the first instance. Staff must not share personal contact details with pupils (mobile telephone numbers, non-work email addresses, social networking sites etc.) unless there is a justifiable reason (e.g. family or friend networks or external groups) and any unintended breach must be reported to the user's line manager immediately. If staff receive contact online from a pupil or ex-pupil they should decline the contact, explaining the safeguarding reasons for this, and they should notify their line manager or Designated Safeguarding Lead.

Confidentiality

Disclosure of confidential information on, or via, social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- the Health and Safety at Work Act 1974
- the Data Protection Act 2018

Staff should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media. Such laws include (but may not be limited to):

- the Libel Act 1843
- the Defamation Acts 1952 and 1996
- the Copyright, Designs and Patents Act 1988

- the Criminal Justice and Public Order Act 1994
- the Protection from Harassment Act 1997
- the Malicious Communications Act 1998
- the Communications Act 2003

It is crucial that staff ensure they are familiar with ACE's Data Protection Policy and this policy and that they do not breach confidentiality when using social media.

Staff must not discuss confidential information relating to ACE on their personal social media sites or accounts. Photographs, videos or any other images which identify ACE premises, pupils or their families, or staff wearing ACE logos must not be placed online on any form of personal social media site. ACE email addresses and other official contact details must not be used either for setting up personal social media accounts or for the facilitation of communication through such media.

Reputation

ACE recognises that staff are entitled to make use of social media in a personal capacity away from work. Staff must be mindful that their online actions can potentially cause damage to the reputation of the organisation if they are identified as being employees of, or as having professional links to ACE. Staff must therefore ensure that if they engage with social media they must do so sensibly and responsibly. They must be confident that any content, comment or opinion expressed through their personal use of social media will not adversely affect, nor be found damaging to, the reputation or credibility of ACE, nor otherwise breach any of ACE's policies. Staff should be aware that, in the event that they access any personal web-based email accounts via the ACE network, those accounts may be subject to ACE's internet monitoring.

Staff must avoid bringing ACE into disrepute and must not use any online (or equivalent) facility to attack or abuse colleagues or service users. Staff are encouraged not to discuss their work on social media, and any views they express should be referred to as their own and not necessarily reflective of their employer's views.

Staff must not edit open access online encyclopaedias (such as Wikipedia) in a personal capacity at work, as the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from ACE itself.

Privacy

Staff must ensure their social media accounts do not compromise their professional position and they should ensure that their privacy settings are set correctly. Staff should also be aware that settings can change, and they should regularly review their list of friends.

Staff are advised to ensure that they set the privacy levels of their personal sites securely and to opt out of public listings on social networking sites in order to safeguard their own privacy.

Staff should keep their passwords confidential, should change them often and should at all times be vigilant about what may or may not legitimately be posted online, and should be aware that it is not safe to reveal home addresses, telephone numbers or other personal information online. Staff are encouraged to be mindful of the risk of fraud and identity theft online and are advised to carefully consider the amount of personal information they display, share or reveal online. Staff should always keep their passwords secret and take all necessary measures to protect access to accounts.

Individuals should remember that by making use of social media they are effectively placing information within the public domain and cannot be reliant on the belief that supposedly 'private' comments or viewpoints will not gain a wider currency or exposure.

Conduct on social networking sites

When using social media, staff must not do anything that may bring ACE into disrepute. Staff are encouraged to think about any photos they may appear in and on social media (e.g. they may wish to 'untag' themselves from a photo). If staff find inappropriate references to themselves and/or images of them posted by a 'friend' online, they are encouraged to contact them and the site to have the material removed.

Staff are reminded that parents and pupils may access their profile and could, if they find the information and/or images it contains offensive, complain to ACE.

If staff have any concerns about information on their social networking sites or if they are victims of cyber-bullying, they should contact their line manager.

Staff must observe all relevant copyright law before posting content that doesn't belong to them.

Caution

Staff are advised to be careful when using social media messaging. For example, as has been found with recent case law, the content of WhatsApp messages can not only lead to the loss of employment but can result in professional disciplinary proceedings against any regulated professionals involved in the behaviour. Case law demonstrates that:

- the private nature of WhatsApp messaging is not a defence.
- any WhatsApp group is only as strong as its weakest member (and any persons they are connected with).
- receiving offensive material via WhatsApp, staying in a group in which it is being circulated and not reporting fellow regulated members can all lead to charges of professional misconduct.

All social media platforms have reporting/take down processes, therefore if staff come across information on a social media platform they wish to be removed, there

are processes for this. However, processes usually involve selecting from a drop down menu (although some allow a form to be completed with narrative provided). Processes are largely operated by bots, and extreme content is normally automatically taken down.

Staff are advised to retain evidence of social media posts that concern them. They are advised to keep a log of problematic social media posts is essential; take screenshots that show the date and time and followers/following (Twitter) or likes/friends/followers (Facebook). For issues with YouTube, staff should download the content recording date, time and number of views. Staff should record all reports or take down requests and set up alerts to enable all content to be monitored and appropriate action taken.

Advice Relating to Facebook Use

As a minimum, ACE recommends the following when staff use Facebook:

Privacy Setting Recommended security level
Send the user messages - friends only
See the user's friend list - friends only
See the user's education and work - friends only
See the user's current city and hometown - friends only
See the user's likes, activities and other connections - friends only
View the user's status, photos, and posts - friends only
Family and relationships - friends only
Photos and videos - friends only
Religious and political views - friends only
Birthday - friends only
Permission to comment on your posts - friends only
Places you check in to - friends only
Contact information - friends only

Users must always make sure they log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/pupils. The user's account can be hijacked by others if the user remains logged in – even if they quit the browser and/or switch the machine off. Similarly, Facebook's instant chat facility means conversations can be viewed later on. Users must ensure they clear their chat history on Facebook (click "Clear Chat history" in the chat window).