

ICT and Social Networking Policy

Approved by:

Board of Trustees

Date:

January 2026

Date of Next Review:

January 2027

SUPPORT
CYBER SECURITY
MULTIMEDIA
COMMUNICATIONS
INFRASTRUCTURE
TECHNOLOGY
CONNECTIVITY
DATA PROTECTION
& INFORMATION SYSTEMS
PERSONAL INFORMATION

OUR VALUES

AMBITION	We instil a lifelong love of learning and nurture skills and talents
INCLUSION	We welcome and respect people from all backgrounds, valuing and celebrating diversity
ASPIRATION	We want people to be the best they can be, and for everyone to achieve their potential
COMMUNITY	We develop local and global citizens for the future, always committed to working in partnership
BELIEF	We encourage everyone to believe in themselves and their future, providing opportunities to excel

Our Vision

Our vision is to make sure all students get the best educational experience. This means that alongside our broad and aspirational curriculum, we offer students diverse enrichment opportunities to help them find their passions.

It's important to us that students grow both academically and personally. To do this, we create safe, inclusive and enriched learning environments in our schools, with opportunities outside of the classroom that open up pathways to successful futures.

We respect each school's individuality and the communities you serve, so we'll work with you to support your development without changing your identity. Our network of schools collaborate and share knowledge to provide exceptional learning experiences and more opportunities for students to find what they love, and what they're good at.

Our Aims

Our aim is to ensure that all schools within the trust aspire to be strong providers and aim for exemplary practice through creative approaches.

Our Future

We strive for continuous improvement and development. Our expansion will create and nurture a strong partnership of schools, covering both primary and secondary phases. Simply put, we believe that we are better, together. Working collaboratively allows us to build on each school's strengths, while supporting areas of improvement.

Our Governance

We have five members who hold the board of trustees to account for the performance of the trust. In addition to the trust board, each member school has its own local Trust.

Contents

	Page
1 Purpose and Scope	04
2 Use of the Achieve and Learn Trust's IT Equipment	05
3 Using Social Media	06
4 Personal Use of Trust / School Owned Devices at Work	06
5 Online Contact with Children and Young People	07
6 Security and Online Identity Theft	08
7 Compliance with the Law	09
8 Privacy and Decency when Online	10
9 Online Bullying and Harassment	10
10 Inappropriate Posting	11
11 Communicating Online on Behalf of The Trust or an Academy	11
12 Monitoring of Online Access at Work	11
13 Disciplinary Implications	12
14 Appendices	
Appendix 1 – Guidelines for Bloggers and Blogging	13
Appendix 2 – Guidelines for Social Networks	14
Appendix 3 – Guidelines for Media Sharing	15
Appendix 4 – Acceptable Use Agreement	16

This policy applies to all staff employed by the Achieve and Learn Trust, at Trust level or in its academies. In addition, the principles pertaining to the policy apply to employees, visitors and volunteers who also have a personal responsibility for their online behaviour and ensuring their use of social networking media takes place within appropriate boundaries and does not bring the individual, the Achieve and Learn Trust or its academies, into disrepute.

A person's social media activities take place completely outside of work, as their personal activities should. However, what they say can have an influence on their ability to conduct their job responsibilities, their work colleagues' abilities to do their jobs, and school's interests and reputation.

This policy sets out the principles which employees of the Achieve and Learn Trust are expected to follow when using the Internet and gives interpretations for current forms of interactivity. The Internet is a fast-moving technology and it is impossible to cover all circumstances, however the principles set out in this document should always be followed.

Facebook, X (formally Twitter), TikTok, Instagram, blogs, YouTube, Blue Sky, Wikipedia and professional networking sites such as LinkedIn are all examples of social media. The term covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations.

Schools are increasingly looking to social media to engage with their audiences. People expect to 'talk back' when organisations communicate with them and they expect that those agencies will in turn respond and do so in appropriate language. Social media enables that kind of interaction to happen in a more efficient manner than, for instance, arranging formal meetings.

Audiences are also becoming fragmented and diverse, the old ways of communicating (for example, by newsletter) are increasingly losing impact. Information needs to be provided in a variety of formats so each target audience can choose how to access it. Photographs can tell a thousand words and videos are very accessible for a wide audience.

- All employees of the Achieve and Learn Trust that use any device owned by the Trust or any of its academies should have read, understood and signed the Acceptable Use Policy (See Appendix 4)
- Employees must protect the security of the I.T networks, systems and information belonging to the Achieve and Learn Trust and it's Academies at all times, as well as being mindful of GDPR regulations.
- Employees must not install any applications without prior permission from the ICT Network Manager
- Employees should not open any emails from senders they do not know and trust, particularly if they have attachments. Such emails should not be forwarded within the Achieve and Learn Trust or Academy unless the employee knows that they are virus free.
- Employees should use the "Report Phishing" button in Microsoft Outlook to submit an email they feel is suspicious for analysis
- Employees should remember that their online activity can be traced back to the Achieve and Learn Trust and its Academies. As such, employees should not engage in any online activity which breaches the ICT Policy or procedures.
- Employees must not reveal any details of any I.T. system or service in use by the Achieve and Learn Trust or its Academies. This includes detailing of software used for Email and Internet access as well as Virus protection.

3

Using Social Media

Achieve and Learn Trust schools operate a physical hardware firewall between their network and the internet as well as a software-based firewall which is configured on all school managed workstations and servers. The purpose of the firewall is to manage the data being transferred to and from a device or network and only allow legitimate and required traffic.

On school owned devices, the firewall is managed by the school's I.T. department. If a user suspects that a firewall is not functioning correctly, they should contact the school's Network Manager.

4

Personal Use of Trust / School Owned Devices at Work

Achieve and Learn Trust and its Academies have developed IT systems to assist employees with their work. We do, however, recognise that there are times when employees may want to use the IT systems for non-work-related purposes and in recognising this need, Achieve and Learn Trust permits employees to use the IT systems for responsible personal use.

If, within the above parameters, employees chose to use the Trust's IT systems to access social networking sites and/or other online forums such as blogs etc. They must do so in a responsible and appropriate manner. There is no unconditional right for an employee to access such sites, and the Trust reserves the right to restrict access to the internet (or certain websites) for employees if there is a cause for concern over their usage.

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private.

Employees are permitted to use installed software packages such as the Microsoft Office suite for responsible and appropriate personal use however employees should be aware that this usage can be monitored and that personal documents should not be stored on Trust or Academy managed storage platforms such as Microsoft OneDrive.

Employees are not permitted to use devices such as Trust or Academy-owned printers and digital cameras or for non-work-related purposes.

Employees are reminded that although the Achieve and Learn Trust permits responsible and appropriate personal use of its IT systems, this must not come as a detriment to their professional obligations to the Trust or Academy. Personal use is only permitted outside of an employee's contracted working hours.

From a safeguarding perspective, there is a widely held concern that social networking may increase the potential for sexual exploitation of children and young people or provide opportunities for “grooming” to take place. It is also possible that those who work with children and young people may be at risk from false allegations being made against them. It is therefore vital that employees use social media responsibly and, with these concerns in mind, take appropriate steps to protect themselves from allegations, maintain appropriate boundaries, exercise appropriate judgement and avoid any contact that may lead to their intent and motivations for any such dialogue to be questioned.

Employees in a school have a duty to safeguard children and young people, and it is therefore inappropriate for employees to communicate via social networking sites with pupils.

Personal devices belonging to employees, such as mobile phones or laptops should never be used by any students or children within the care and trust of an Achieve and Learn Trust academy.

Specifically, in respect of social media, employees of the Achieve and Learn Trust should not share personal information with children / young people and must not become “connected” with any child or young person to whom they have acted in a position of trust. It would be recommended that the same approach is taken with parents. Extreme care must be exercised when using social media sites to establish the identity of “followers” and when using online chat rooms as it may be difficult to ascertain to whom you may be chatting. Should a young person attempt to contact an employee of the Achieve and Learn Trust via social media, this should be reported to the employee’s line manager immediately.

Any inappropriate conduct in relation to online communication with children and young people will be taken extremely seriously and investigated in line with safeguarding and / or the Achieve and Learn Trust’s Disciplinary Procedures.

Employees are reminded to be IT security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites and online forums allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which may form the basis of security questions and passwords.

Employees must take care when posting such information, in order that it does not allow a breach of IT security within any Achieve and Learn Trust academy or raise the possibility of the employee's online identity being stolen.

Employees are advised to think carefully about who they give out personal details to, like home addresses, phone numbers, financial information or full date of birth, to prevent online identity theft.

In addition, employees should:

- Ensure no information is made available that could provide a person with unauthorised access to an Achieve and Learn Trust academy and/or any confidential information belonging to the school, its employees, students and/or members of the public; and
- Refrain from recording any confidential information regarding Achieve and Learn Trust or its academies, employees, students and/or members of the public on any social networking website.

Employees should note that if they are found to have posted confidential material regarding Achieve and Learn Trust or its academies in any format online, they are required to assist in any way to ensure such material is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

Employees are required to always stay within the law when communicating online. They need to be aware that fair use, financial disclosure, libel, defamation, copyright and GDPR apply on-line, just as they do in any other form of the media.

Libel: If a person publishes an untrue statement about another person which is damaging to their reputation, the latter may take a libel action against them. This will also apply if that person allows someone else to publish something libellous on their website if they know about it and don't take prompt action to remove it. A successful libel claim against a person will result in an award of damages against them.

Copyright: Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc.) which without permission is likely to breach copyright laws. Employees should avoid publishing anything they are unsure about or seek permission in advance. Breach of copyright may result in an award of damages against that person.

GDPR: All employees should have an up-to-date certificate of GDPR compliance training.

Obscene material: It goes without saying that employees should avoid publishing anything that people would consider obscene. Publication of obscene material is a criminal offence.

In addition, a person who posts grossly offensive or indecent material may be found to be guilty of an offence under the Communications Act 2003.

Employees must at all times remember their responsibilities to Achieve and Learn Trust, its parents/carers, students and colleagues, and never give out details of or divulge dealings with colleagues, parents or students without their explicit consent. Employees should check with their manager if they are not sure what is and is not confidential.

Employees must not use slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace which could bring the Achieve and Learn Trust or any of its academies into disrepute, break the law and/or leave the employee open to prosecution and/or disciplinary action.

Employees are encouraged to be themselves, but to be considerate about other people's views, especially around contentious topics.

Employees are encouraged to be credible, accurate, fair and thorough and ensure they are doing the right thing.

Employees are encouraged to share useful information that they gain from using social media with others, where appropriate.

Social media does have potential dangers and drawbacks. In society in general, adults, as well as children, have found themselves the target of online abuse, bullying and harassment (cyber-bullying), including name calling/ malicious comments, exclusion, intimidation, spreading of rumours, or bombarding with unwanted messages.

Bullying or harassment of any kind, including using online channels is totally unacceptable and will not be tolerated. Cyber-bullying can have a significant impact upon the health, wellbeing and confidence of those targeted, and because technology is accessible 24/7, it can impact upon an individual's private life.

Support is available for any employees who feel they have been bullied or harassed via social networking sites through their Trade Union representative and HR, as well as in school. In the first instance, staff should refer any cyber bullying concerns to the Headteacher, who will be able to provide information and guidance.

All complaints regarding bullying or harassment will be treated extremely seriously.

10

Innapropriate Posting

If an employee is found to have posted inappropriate material in any format on the internet, they will be required to assist in any way to ensure such material is removed without delay.

Staff should remember that colleagues and parents/carers may see their online information.

Whether they identify themselves as an employee of the Achieve and Learn Trust or not, staff are encouraged to think carefully about how much personal information they want to make public and make sure their profile and the information they post reflect how they want themselves to be seen, both personally and professionally.

11

Communicating Online on Behalf of the Achieve and Learn Trust or an Academy

Employees should not comment on behalf of the Achieve and Learn Trust or its Academies (disclose information, publish information, make commitments or engage in activities on behalf of the Achieve and Learn Trust or its Academies), unless they are specifically authorised to do so by the CEO of the Trust, Headteacher of the Academy and/or the Chair of Governors. If not specifically authorised to do so, they should speak to the CEO or Headteacher before taking any action. Remember employees are personally liable for what they publish online.

12

Monitoring of Online Access at Work

Employees should be aware that, in order to protect its legitimate business interests and its IT systems, Achieve and Learn Trust academies reserve the right to monitor internet use in accordance with the provisions set down in the school's IT Policies and Procedures.

If the Achieve and Learn Trust finds that an employees' internet use is not in accordance with this policy, access to the internet through school's IT systems may be withdrawn.

Employees must be aware that if they do not adhere to this policy, disciplinary action may be taken in line with the Achieve and Learn Trust's Disciplinary Procedure. If deemed sufficiently serious, this could result in dismissal.

Appendix 01 – Guidelines for Bloggers and Blogging

1. If an employee already has or plans to have a personal blog or website which shows in any way in that they work within the Achieve and Learn Trust or its academies, they must tell their Headteacher. They should include a simple and visible disclaimer such as “The views expressed here are my own and don’t necessarily represent the views of Achieve and Learn Trust”).
2. If an employee thinks that something on their blog or website may cause a conflict of interest, or they have concerns about impartiality or confidentiality, they should speak to the Headteacher of their academy or the CEO if the employee works on the Trust Central Team. If in any doubt, employees should not talk about what they do at work.
3. If someone offers to pay an employee for blogging, this could cause a conflict of interest and the Headteacher or CEO must be consulted.

Appendix 02 – Guidelines for Social Networks

This section covers Social Networks, Discussion Forums, Wikis etc.

1. Employees should use their best judgment, remembering that there are always consequences to what is published.
2. Employees should not use their Achieve and Learn Trust or Academy email account or work number in on-line discussions unless they have been authorised to speak for the school/Trust.
3. It is not a good idea to invite parents/carers to become friends on social networking sites. There may be a conflict of interest, the blurring of boundaries, security and privacy issues.
4. Make sure any wiki entries, articles or comments are neutral in tone, factual and truthful.
5. Never post rude or offensive comments on any online encyclopaedias.
6. Before editing an online encyclopaedia entry about the Achieve and Learn Trust or its academies, or any entry which might cause a conflict of interest, or adding links, check the house rules of the site. Permission may be required from the relevant wiki editor and the Headteacher.
7. It is important to respond to legitimate criticism with facts, but speak to the Headteacher for advice before responding; a poor response could make matters worse. Never remove criticism of the Achieve and Learn Trust or it's academies or derogatory or offensive comments. Report them to the Headteacher or CEO for them to act.

Appendix 03 – Guidelines for ‘Media’ Sharing (Video, Photos, Presentations etc.)

1. Make sure all video and media are safe to share, do not contain any confidential or derogatory information, and are not protected by any copyright, or intellectual property rights.
2. If the content is official Achieve and Learn Trust or Academy content, then it must be labelled and tagged as such.
3. Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: “This is my personal work and does not necessarily reflect the views of Achieve and Learn Trust”).

Appendix 04 – Acceptable Use Agreement: Staff, Governors, Trustees and Visitors

This Acceptable Use Policy is intended to ensure:

- That staff, governors and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That Achieve and Learn Trust or Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

Achieve and Learn Trust will try to ensure that staff, governors and visitors will have good access to ICT to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the Achieve and Learn Trust's and its academies ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand and consent that the Achieve and Learn Trust or its academies may monitor and record my use of ICT systems for the purpose of ensuring that rules are being complied with and for legitimate business purposes. The email system will only be monitored for a particular user by direct request from the Headteacher / CEO or Senior Leadership Team member.
- I understand that the Achieve and Learn Trust and its Academies ICT systems are primarily intended for educational use and I will only use the Trust or Academy's email / Internet / Intranet / Remote Access etc. and any related technologies for professional purposes.
- I will not install any hardware or software onto the Achieve and Learn Trust or its Academies system (including school laptops) without permission.
- I understand that the rules set out in this agreement also apply to use of the Achieve and Learn Trust and its Academies ICT systems (e.g. laptops, email, remote access etc.) outside of the Achieve and Learn Trust and its Academies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Headteacher/designated SLT member or CEO.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that if I take and/or publish images of others I will do so with their permission and in accordance with GDPR. I will not use my personal equipment to record these images, unless I have permission to do so. (Staff may obtain permission from the Headteacher/Designated member of SLT to use specific equipment on each occasion where the equipment will be used). Where these images are published (e.g. on the Achieve and Learn Trust or Academy website / social media) it will not be possible to identify by name, or other personal information, those who are featured. There may be occasions where this rule cannot be applied, e.g. in newspaper articles, Academy newsletters and bulletins. In the event of this, prior approval should be obtained from the Headteacher.
- I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner. I will not communicate confidential information by e-mail.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will abide by the latest GDPR regulations at all times.

All staff, Governors and Trustees have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- If I use my personal handheld / external devices (iPad / laptop / Smartphone etc) that connect to the Trust or academy network, I will follow the rules set out in this agreement, in the same way as if I was using Trust or academy equipment. I will also follow any additional rules set by the Achieve and Learn Trust about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- The Achieve and Learn Trust or academy will provide staff with an email account. This account is to be used for Achieve and Learn Trust or academy business only.
- Staff must not use their work email account for personal banking, online shopping etc. Access to personal email accounts (i.e. hotmail, gmail etc) using the Achieve and Learn Trust or academy system is authorised, but staff are strongly advised that they must not use their personal email account to contact parents, carers, students etc.
- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Data relating to Achieve and Learn Trust's or academy business must only be stored on Trust or academy managed systems. External USB storage devices should not be used unless explicit permission is given in writing by the headteacher / CEO, in which case the device must be encrypted using a trusted encryption method such as BitLocker before being used.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to

others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the Achieve and Learn Trust's or the Academy's policies.
- I will not disable or cause any damage to Trust or Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, when it abides by GDPR regulations and/or I am required to by law.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Achieve and Learn Trust or it's Academie's sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of Achieve and Learn Trust and its Academies relating to this policy.
- I understand that this Acceptable Use Policy applies not only to my work and use of Achieve and Learn Trust's or its academies ICT equipment in school but also applies to my use of Achieve and Learn Trust's or its academies ICT systems and equipment outside of school.
- I understand that this Acceptable Use Policy applies to my use of personal equipment in Achieve and Learn Trust's or its academies or in situations related to my employment by the Achieve and Learn Trust.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the information contained above and understand that this information has been formulated as an overview and should be read in conjunction with the full ICT Acceptable Use Policy and the social media policy contained on the following pages and that I agree to use the Achieve and Learn Trust's or its academies ICT systems (both in and out of the Achieve and Learn Trust or its academies) and my own devices.

Staff Name: _____

Signed: _____

Date: _____