A CHURCH OF ENGLAND MULTI-ACADEMY TRUST
DEDICATED TO TRANSFORMING CHILDREN'S LIVES

Colossians 3:12 Therefore, as Gods chosen people, holy and dearly loved, clothe yourselve with compassion, kindess, humility, gentleness, and patience.

Document Title	**ICT User and Social Media Policy**
Author/Owner (Name and Title)	Laura Lowe, Director of Colleague Services
Version Number	V1
Date Approved	26th June 2025
Approved By	LAAT Board

Policy Category 1	**1**	**Trust/Academies to use without amendment**
	2	Academy specific appendices
	3	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V1	June 2025	LL	Reviewed in consultation with recognised Trade Unions. No sigificant changes to note.

About this policy

- This policy applies to all employees, governors, volunteers, visitors and any contractors using our ICT facilities (referred to henceforth as 'Employees'). Ensuring ICT is used correctly and properly, and that inappropriate use is avoided is the responsibility of every employee. If employees are unsure about any matter or issue relating to this policy, they should speak to their line manager or Headteacher/Executive Headteacher.

- The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT provided by the Trust to protect the Trust, pupils and its employees from risk. We recognise that the use of ICT also enhances teaching and learning and this policy provides a framework for this to be carried out safely.

- IT and communications systems are intended to promote effective communication and working practices. This policy outlines the Trust's standard requirements that employees must observe when using these systems, the exceptional circumstances in which the Trust or school may monitor an employee's use, and the action that may be taken in respect of breaches of these standards.
- The policy also provides advice and guidance to our employees on the safe use of social media. The acceptable use of ICT and Social Media will be covered during induction and ongoing training will be provided, as appropriate.
- Breach of this policy may be investigated in line with the Trust's Disciplinary Procedure
- This policy has been implemented following consultation with recognised trade unions.
- The Trust use MFS (Multi Factor Authentication) across its systems and employees will be expected to comply with these security requirements.

Equipment security and passwords

- Employees are responsible for the security of the equipment allocated to or used by them and should use strong passwords on all IT equipment, particularly items that are used away from any Trust or school premises.
- Employees should keep passwords confidential and change them regularly.
- Employees must only log on to any Trust systems using their own username and password.
- If employees are away from their device, they should log out or lock it.

Systems and data security

- Employees should not delete, destroy or modify existing systems, programs, information or data except as authorised in the proper performance of their duties or in order to comply with this Policy following an instruction from a designated manager.
- Employees must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to any Trust or school systems without authorisation from the Headteacher/Executive Headteacher or their Manager. All removable media devices should be encrypted. The use of removable media devices for the storage or transferring of personal or sensitive data is not permitted (see Data Protection Policy).
- All systems are monitored for viruses. If an email looks suspicious employees must not reply to it, open any attachments or click any links in it.

- Employees should inform their Headteacher/Executive Headteacher or IT Services immediately if they suspect their computer may have a virus.
- Employees should not send out sensitive data through email unless the information is encrypted or password protected.

Email

- Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails from equipment provided for work by the Trust. Please also see section relating to Social Media in relation to sites accessed for personal use on own devices.
- Employees should adopt a professional tone and observe appropriate etiquette when communicating by email.
- Employees should remember that emails can be used in legal proceedings and may be required in response to Subject Access Requests, and that even deleted emails may remain on the system and are capable of being retrieved.
- Employees must not:
    a) send, forward or read private emails at work which employees would not want a third party to read
    b) send or forward chain mail, junk mail, cartoons, jokes or gossip.
    c) send messages from another person's email address (unless authorised) or under an assumed name.
- Employees should consider whether it necessary to send an email and consider the workload impact of the recipient/whether a phone call would be more appropriate.
- Employees must not use their own personal email account to send or receive email for the purposes of the Trust or school's business. Only use the email account provided for employees.

Using the internet

- Internet access is provided primarily for Trust and school business purposes.
- Personal use should be limited to breaks and lunch periods, unless there is an emergency and the Headteacher/Line Manager should be made aware.
- Employees should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition.
- The Trust or school will block or restrict access to some websites at their discretion.

Monitoring

- We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Trust or school, including for the following purposes (this list is not exhaustive and may include messages or postings on all social media platforms): -
    a)
    b) To assist in the investigation of alleged wrongdoing
    c) To comply with any legal obligations.
    d) To assist in the investigation of any Safeguarding concern/cases

Prohibited use of the Trust's Systems

- Misuse or excessive personal use of the school's systems or inappropriate internet use may be investigated in line with our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence. In the case of visitors or outside agencies, it may be necessary to contact the employer.
- Using Trust or School email systems or internet for the following purposes is prohibited (this list is not exhaustive): -

  a) Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit nature)

  b) Offensive, obscene or criminal material or material which is liable to cause embarrassment to the Trust or school or any stakeholders

  c) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy)

  d) Confidential information about the Trust, our schools, or any of our staff, pupils or stakeholders (except as authorised in the proper performance of an employee's duties)

  e) Unauthorised software

  f) Any other statement which is likely to create any criminal or civil liability (for employees of the Trust or any school)

  g) Music or video files or other material in breach of copyright

This does not prevent the employee from blowing the whistle and making a disclosure in the public interest.

Personal Devices

- All personal devices must be switched off or put on silent mode whilst teaching or supervising pupils on any Trust or school premises and during the course of normal duties. In line with the staff Code of Conduct, any personal equipment capable of photographing children should be stored securely during the school day and such items should not be taken into the classroom in line with safeguarding requirements. Use of personal devices is normally restricted to breaks and lunch periods or outside of the school/working day only and must not be used, unless agreed by the Headteacher/Executive Headteacher, during contact with pupils.
- No employee will be required to use their personal device for professional/business use. Where employees are required to use a device for professional purposes (such as a school trip or visit) one will be provided by the employer.

Social Media

- This section deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram, Tumblr and all other social media networking sites, internet postings and blogs. It applies to use of social media for Trust or school purposes as well as personal use that may bring the Trust into disrepute.
- It is strongly advised that personal profiles on social media sites are set to 'private, always using the highest security setting'.
- The use of social media for personal purposes is not normally permitted during working hours and is restricted to breaks and lunch periods/PPA or non contact time or outside of the working day. See 'Personal Devices' above.
- Employees may use personal social media accounts for professional purposes (such as LinkedIn and Twitter) however, caution should be exercised when noting affiliation with the school or Trust and employees must ensure use complies with this policy.

- Employees must avoid making any social media communications that could damage our business interests or reputation, even indirectly. (Please see the Staff Code of Conduct).
- Employees must not use social media to defame or disparage the Trust, any school, our staff or pupils or any third party; to harass, bully or unlawfully discriminate against staff; to make false or misleading statements; or to impersonate colleagues or third parties.
- Employees must not express or post opinions on the Trust or any school's behalf via social media, unless expressly instructed to do so in the course of their job role.
- Employees must not post comments about sensitive Trust or school related topics, such as the school or Trust's performance, or do anything to jeopardise sensitive Trust or school information, confidential information or information relating to pupils or staff. Employees must not include our logos in any personal social media posting or in their personal profile on any social media unless they have written permission to do so from their line manager.
- Employees should be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see and that what they publish might be available to be read by the masses, including the employer, in the future as well as the present. Employees should also be aware that once an image or post has been shared on social media they may lose control of that posting.
- If employees are uncertain or concerned about the appropriateness of any statement or posting which may relate to the school or the Trust, refrain from posting it until it has been discussed with their line manager or Headteacher/Executive Headteacher.
- Employees should report any social media content that disparages or reflects poorly on the Trust or any school to their line manager. Employees should ensure that social media profiles and their content are consistent with the professional image they present to students, colleagues and their employer.
- Employees should be extremely cautious when using social networks outside of school. It is strongly advised that no contact should be made with pupils, their families and or carers, except in exceptional circumstances and with the awareness of the Headteacher. This is with the exception of legitimate personal relationships created independently of work which may include family members and, where there is a genuine need, the children of close friends.
- Any misuse of social media should be reported to the employee's line manager, Headteacher/Executive Headteacher in the first instance. In the case of safeguarding concerns, misuse should be reported to the individual school's DSL.
- Any inappropriate contact via social media channels e.g. for a work matter raised on personal social media should be communicated to line managers. This should also apply in instances of inappropriate contact via social media from a student. Employees should be aware that it may be appropriate for both of them to be dealt with under the Safeguarding Policy.

Breaches of this policy

- Breaches of this policy may be investigated in line with disciplinary policy.
- Employees may be asked to remove any social media content that we consider to constitute a breach of this policy.