



Leigh Academy
Strood

Leigh Academy Strood

ICT and Acceptable Use Policy

Academic year 2025/26

Date of issue	September 2025
Date to be revised	August 2026

Leigh Academy Strood ICT and Acceptable Use Policy

Introduction and aims

Information and communications technology (ICT) are an integral part of the way our academy works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academy.

However, the ICT resources and facilities our academy uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the academy community engage with each other online
- Support the academy's policy on data protection, online safety and safeguarding
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching pupils safe and effective internet and ICT use

This policy covers all users of our academy's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policy and staff code of conduct.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- [The General Data Protection Regulation](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [The Education and Inspections Act 2006](#)
- [Keeping children safe in education 2025](#)
- [Searching, screening and confiscation: advice for schools](#)

- [National Cyber Security Centre \(NCSC\)](#)
- [Education and Training \(Welfare of Children Act\) 2021](#)

Definitions

- “ICT facilities”: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- “Users”: anyone authorised by the academy to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- “Personal use”: any use or activity not directly related to the users’ employment, study or purpose
- “Authorised personnel”: employees authorised by the academy to perform systems administration and/or monitoring of the ICT facilities
- “Materials”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

Unacceptable use

The following is considered unacceptable use of the academy’s ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the academy’s ICT facilities includes:

- Using the academy’s ICT facilities to breach intellectual property rights or copyright
- Using the academy’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the academy community

- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the academy
- Using websites or mechanisms to bypass the academy's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The academy reserves the right to amend this list at any time. The Principal will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

Exceptions from unacceptable use

Where the use of academy ICT facilities (on the academy premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion.

Approval can only be granted by the Principal and network manager. This must be requested through the IT helpdesk.

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the academy's policies on behaviour and staff code of conduct.

Staff (including governors, volunteers, and contractors)

Access to academy ICT facilities and materials

The academy's network manager manages access to the academy's ICT facilities and materials for academy staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the academy's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network manager.

Use of phones and email

- The academy provides each member of staff with an email address.
- This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.
- All work-related business should be conducted using the email address the academy has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the James Root immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the academy to conduct all work-related business.

- academy phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The network manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- Staff may not use the academy's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).
- Staff should be aware that use of the academy's ICT facilities for personal use may put personal communications within the scope of the academy's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the staff Code of conduct
- Staff should be aware that personal use of ICT (even when not using academy ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Academy social media accounts

The academy has an official Facebook page, managed by Mr Fatania and James Roots. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The academy has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of academy network and use of ICT facilities

The academy reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The academy monitors ICT use in order to:

- Obtain information related to academy business
- Investigate compliance with academy policies, procedures and standards
- Ensure effective academy and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Pupils

Access to ICT facilities

- All students have their own Chromebook
- Computers and equipment in the academy's ICT rooms are available to pupils under the supervision of staff
- Specialist ICT equipment e.g. for music, photography and design technology can only be used under the supervision of staff

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the academy has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under academy rules or legislation. Please see Behaviour Policy for more information.

The academy can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the academy's rules. Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of academy

The academy will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on academy premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, other pupils, or other members of the academy community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Parents

Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course.

However, parents working for, or with the academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the academy's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the academy online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the academy through our website and social media channels.

Data security

The academy is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the academy cannot guarantee security. Staff, pupils, parents and others who use the academy's ICT facilities should use safe computing practices at all times.

The academy uses smoothwall as a monitoring and filtering tool, this will notify the safeguarding team of students who are using technology inappropriately and they will be sanctioned accordingly. This system also identifies students who may require further support from our safeguarding/pastoral team.

Passwords

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Software updates, firewalls and anti-virus software

All of the academy's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the academy's ICT facilities.

Any personal devices using the academy's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the academy's data protection policy.

Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to academy systems, files and devices.

These access rights are managed by the network manager

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert James Roots immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption

The academy ensures that its devices and systems have an appropriate level of encryption.

academy staff may only use personal devices (including computers and USB drives) to access academy data, work remotely, or take personal data (such as pupil information) out of academy if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network manager.

Protection from cyber attacks

The academy will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the academy secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the academy's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
 - Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
- 'Proportionate': the academy will verify this using a third-party audit from the Trust network team, at least annually, to objectively test that what it has in place is up to scratch
- Multi-layered: everyone will be clear on what to look out for to keep our systems safe
- Up-to-date: with a system in place to monitor when the academy needs to update its software
- Regularly reviewed and tested: to make sure the systems are as up to scratch and secure as they can be
- Make sure staff:
- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where they can, on things like academy email accounts
- Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the academy has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the academy will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested several times throughout the year and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Leigh Academy Strood works with the Leigh Academies trust to prevent cyberbullying by educating staff and students.

Internet access

The academy wireless internet connection is secured.

The academy uses filtering and connections are different for students and staff. However if inappropriate sites are identified then staff should report this to the IT team at helpdesk@latrust.org.uk and the safeguarding team if searches by students are inappropriate

Pupils

All pupils have their own Chromebook therefore have access to the Wi fi to for learning, however smoothwall filtering and monitoring security measures are in place to avoid inappropriate use of devices. If students search inappropriate content then the safeguarding team is notified immediately due to the security measures set up. They are sanctioned appropriately or provided with additional support from the pastoral/safeguarding team.

Parents and visitors

Parents and visitors to the academy will not be permitted to use the academy's Wi-Fi unless specific authorisation is granted by the Principal.

The Principal will only grant authorisation if:

- Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the academy's WI-FI in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review

The Principal and the IT manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the academy.

This policy will be reviewed every year.

Related policies

This policy should be read alongside the academy's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff conduct
- Data protection
- Artificial Intelligence

Summary of the Acceptable use of technology for students

Learner Acceptable Use of Technology

I understand that the academy Acceptable Use Policy will help keep me safe and happy online at home and at academy.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I will follow the Google Classroom rules that my teacher has shared with me.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher or learning support assistant has chosen.
- I use academy devices for academy work unless I have permission otherwise.
- All Remote Learning will take place via the Google Classroom.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them. 4
- I will not access or change other people's files or information
- I will only change the settings on a device if a member of staff has allowed me to.

Understand

- I understand that the academy internet filter is there to protect me, and I will not try to bypass it.

- I know that all academy devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit childline to learn more about being safe online.
- I know that if I do not follow the academy rules then my access to technology could be taken away or I may receive a consequence in line with the academy's behaviour policy/code of conduct

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to an adult.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.