Leigh Academy Mascalls ICT and Acceptable Use Policy (Academic Year 2025/26)

Date of issue: September 2025
Date to be revised: August 2026

1. Introduction and Aims

Information and communications technology (ICT) is an integral part of Leigh Academy Mascalls, supporting teaching, learning, pastoral, and administrative functions. However, ICT resources 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 online engagement within the academy community.
- Support the academy's policies on data protection, online safety, and safeguarding.
- Prevent disruption 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 the academy's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors. Breaches may be dealt with under the academy's behaviour policy and staff code of conduct.

2. Relevant Legislation and Guidance

This policy complies with:

- Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- 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

3. Definitions

Term	Definition
ICT Facilities	Includes all facilities, systems, and services (network, computers, laptops, phones, software, websites, etc.) 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 user's 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 (documents, photos, audio, video, web pages, social networking sites, and blogs).

4. Unacceptable Use

The following is considered unacceptable use of the academy's ICT facilities by any member of the academy community. Breaches may result in disciplinary or behaviour proceedings.

Unacceptable use includes:

- Breaching intellectual property rights or copyright.
- Using ICT facilities to **bully or harass** someone, or to promote unlawful discrimination.
- Breaching academy policies or procedures.
- Any illegal conduct, or statements 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).

- Activity which defames or disparages the academy or risks bringing it into disrepute.
- Sharing confidential information about the academy, its pupils, or other members of the community.
- Connecting any device to the network without approval from authorised personnel.
- Setting up any software, applications, or web services without approval, or creating/using programs designed to interfere with ICT facilities, accounts, or data.
- Gaining, or attempting to gain, unauthorised access to restricted areas or password-protected information.
- Allowing, encouraging, or enabling others to gain unauthorised access.
- Causing intentional damage to ICT facilities.
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission.
- Causing a **data breach** by accessing, modifying, or sharing data (including personal data) without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business (unless directly related to the academy).
- Using mechanisms to bypass the academy's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory.

The Principal reserves the right to use professional judgement to determine if any act not on this list is considered unacceptable use.

Exceptions from Unacceptable Use

Exemptions may be granted at the **Principal's discretion** and must be approved by the Principal and Network Manager through the IT helpdesk.

Sanctions

Pupils and staff who breach this policy may face disciplinary action in line with the academy's policies on behaviour and staff code of conduct.

5. Staff Use of ICT Facilities and Materials

Access and Log-in

- The Network Manager manages access permissions.
- Staff are provided with **unique log-in/account information and passwords** that must be used.
- Staff must contact the Network Manager to report unauthorised file access or to update permissions.

Use of Phones and Email

- Staff are provided with an academy email address for **work purposes only** and must enable **multi-factor authentication**.
- All work-related business must use the academy email address.
- Staff **must not share personal email addresses or phone numbers** with parents and pupils, nor send work-related materials using personal accounts.
- Staff must take care with email content (to avoid claims for discrimination, harassment, defamation, etc.).
- All emails are potentially retrievable, even after deletion.
- Sensitive or confidential information in email attachments **should be encrypted**.

- If an email containing personal information is sent in error, inform **Adelle King** immediately and follow the data breach procedure.
- Academy phones must not be used for personal matters.

Personal Use

Staff are permitted to **occasionally** use academy ICT facilities for personal use provided it:

- Does not take place during teaching time.
- Does not constitute 'unacceptable use'.
- Takes place when **no pupils are present**.
- Does not interfere with jobs or prevent others from using facilities for work/educational purposes.
- Staff may not use academy ICT facilities to store personal non-work-related information (music, videos, photos).
- Staff should be aware that personal use may be within the scope of the academy's monitoring activities.
- Staff can use personal devices (phones/tablets) in line with the staff Code of Conduct.

Academy Social Media Accounts

The official Facebook page is managed by **Mrs Relf**. Unauthorised staff must not access or post to the account. Authorised staff must abide by academy guidelines for content.

Monitoring of Academy Network

The academy reserves the right to monitor the use of its ICT facilities and network, including: internet sites visited, bandwidth usage, email accounts, telephone calls, user activity/access logs, and any other electronic communications.

Monitoring is carried out by authorised ICT staff to:

- Obtain information related to academy business.
- Investigate compliance with policies.
- Ensure effective academy and ICT operation.
- Conduct training or quality control.
- Prevent or detect crime.
- Comply with legal obligations (e.g., subject access requests).

6. Pupils

Access to ICT Facilities

- All pupils have their own **Chromebook**.
- Computers in ICT rooms and specialist equipment (music, photography, design technology) are available under **staff supervision**.

Search and Deletion

- The academy has the right to search pupils' phones, computers, or other devices for banned data or items (e.g., pornographic images) under the Education Act 2011.
- The academy can and will **delete files and data** found on searched devices if it is believed the data

could disrupt teaching or break academy rules.
- Staff may confiscate devices for evidence to hand to the police if abuse with an online element is disclosed.

Unacceptable Use of ICT and the Internet Outside of Academy

The academy will sanction pupils, in line with the behaviour policy, if they engage in unacceptable use (as defined in Section 4) **at any time**, even if not on academy premises.

7. Parents

Access to ICT Facilities and Materials

- Parents do not have access to the academy's ICT facilities as a matter of course.
- Parents working in an official capacity (volunteer, PTA member) may be granted appropriate access at the headteacher's discretion, and **must abide by the staff rules in this policy**.

Communicating Online

Parents play a vital role in modelling respectful online communication when interacting with the academy through its website and social media channels.

8. Data Security

Passwords

- All users must set **strong passwords** and keep them secure.
- Users are responsible for the security of their passwords and accounts.
- Staff will use a **password manager**. Teachers will generate and securely store passwords for pupils.

Software Updates, Firewalls and Anti-virus Software

- Academy devices will be configured to perform regular or automatic software/security/anti-virus updates.
- Users must not attempt to circumvent safeguards.
- Any personal devices using the academy's network must also be configured with appropriate security measures.

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

- Users have clearly defined access rights managed by the Network Manager.
- Users should not access or attempt to access systems/files/devices they haven't been granted access to.
- Users must **always log out of systems and lock their equipment** when not in use. Equipment and systems should be closed down completely at the end of each working day.

Encryption

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

- Staff may only use personal devices to access academy data or work remotely if specifically authorised by the headteacher, and only if those devices have appropriate levels of security and encryption as defined by the Network Manager.

Protection from Cyber Attacks

The academy will:

- Provide annual training for staff on cyber security basics (checking email senders, responding to requests for bank details/logins, verifying payment requests).
- Investigate whether IT software needs updating or replacing to be more secure.
- Work with the Trust network team to verify security using a third-party audit at least annually.
- Maintain a multi-layered, up-to-date system to monitor security.
- Ensure staff dial into the network using a **Virtual Private Network (VPN)** when working from home.
- Enable multi-factor authentication where possible.
- Ensure ICT staff conduct regular access reviews.
- Have a firewall in place.
- Check that its supply chain is secure.
- Develop, review, and test an incident response plan.
- Leigh Academy Mascalls works with the Leigh Academies Trust to prevent cyberbullying.

Internet Access

- The academy's wireless connection is secured.
- The academy uses **Smoothwall** as a monitoring and filtering tool to notify the safeguarding team of inappropriate student technology use.
- Staff must report inappropriate sites to the IT team at helpdesk@lattrust.org.uk or the safeguarding team.

9. Learner Acceptable Use of Technology

Pupils understand that the Acceptable Use Policy helps keep them safe and happy online at home and at academy.

Safe

- Behave online the same way as in the classroom.
- Only send messages that are polite and friendly.
- Only post pictures or videos if they are safe, appropriate, and with permission.
- Only talk with and open messages from people they know.
- Only click on links if they know they are safe.
- If someone online suggests meeting up, immediately talk to an adult.

Learning

- Follow Google Classroom rules shared by the teacher.
- Always ask permission from an adult before using the internet.
- Only use websites and search engines that the teacher or learning support assistant has chosen.
- Use academy devices for academy work unless there is permission otherwise.
- All Remote Learning will take place via the Google Classroom.

Trust

- Know that not everything or everyone online is honest or truthful.
- Check content on other sources like other websites, books, or a trusted adult.
- Always credit the person or source that created any work, images, or text used.

Responsible

- Keep personal information safe and private.
- Keep passwords safe and do not share them.
- Will not access or change other people's files or information.
- Only change the settings on a device if a member of staff has allowed it.

Understand

- Understand that the academy internet filter is there for protection, and will not try to bypass it.
- Know that all academy devices and systems are monitored to help keep pupils safe, including when used at home.
- Have read and talked about these rules with parents/carers.
- Can visit Childline to learn more about being safe online.
- Know that if they do not follow the rules, access to technology could be taken away or they may receive a consequence in line with the academy's behaviour policy/code of conduct.

Tell

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