Acceptable Use of ICT and Internet Policy

Policy in effect from: April 2026

Review Date: April 2029

1. Statement of Intent

Mighty Oaks Academy Trust recognises that information and communication technology (ICT) plays an essential role in teaching, learning and the efficient running of the school. Staff and pupils rely on ICT systems and electronic devices to support educational outcomes, communication and administration.

The Trust acknowledges that both school-owned and personal electronic devices are commonly used by staff. This policy sets out clear expectations to ensure ICT is used safely, responsibly and legally, protecting pupils, staff and the school.

This policy aims to ensure that:

- Staff are responsible, safe and professional users of ICT
- School systems and data are protected from misuse, loss or breach
- Pupils are safeguarded when ICT is used
- Clear arrangements are in place for monitoring, security, loss or damage of devices

This policy should be read alongside the Online Safety Policy, Social Media Policy, Safeguarding and Child Protection Policy, Data Protection Policy and Disciplinary Policy.

2. Legal Framework

This policy has due regard to relevant legislation and statutory guidance, including:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000

- Human Rights Act 1998
- Voyeurism (Offences) Act 2019

3. Roles and Responsibilities

Trust Board

The Trust Board has overall responsibility for ensuring the effective implementation and review of this policy.

Head of School

The Head of School is responsible for:

- Implementing and enforcing this policy
- Ensuring staff are aware of monitoring arrangements
- Approving the use of personal devices for work purposes
- Investigating breaches and handling complaints
- Ensuring proportionate use of monitoring systems, including SENSO

ICT Technician

The ICT Technician will:

- Monitor networks, systems and logs for security and safeguarding purposes
- Maintain filtering, antivirus and security software
- Carry out authorised security checks on devices
- Support staff with approved ICT use
- Report data breaches immediately to the Data Protection Officer (DPO)

Data Protection Officer (DPO)

The DPO will:

- Ensure encryption and security of devices
- Provide advice on GDPR compliance
- Support breach response and reporting

Staff

All staff are responsible for:

- Using ICT safely and professionally
- Protecting confidential information
- Reporting misuse or concerns immediately
- Signing and complying with the Device User Agreement

4. Acceptable Use

ICT facilities and devices may be used for legitimate school purposes, including:

- Teaching and learning activities
- School administration and communication
- Approved research and professional development

Staff must:

- Use devices in line with safeguarding and data protection requirements
- Act as positive role models for pupils
- Ensure pupils follow pupil acceptable use agreements

Staff must not:

- Use ICT to access illegal, inappropriate or harmful content
- Communicate with pupils or parents via personal devices or social media
- Bypass filtering or security systems

- Share passwords or user accounts

Any misuse may result in disciplinary action, up to and including dismissal, in line with the Disciplinary Policy.

5. Monitoring and Privacy

The school monitors ICT use to:

- Safeguard pupils
- Protect data and systems
- Ensure compliance with this policy

Monitoring will always be lawful, proportionate and for safeguarding or security purposes.
Access to personal devices will only be undertaken with informed consent and only where necessary.

6. Email and Internet Use

- School email accounts must be used for school business only
- Emails must be professional and appropriate
- Confidential information must be protected (e.g. initials where appropriate)
- Emails are retained in line with the Records Management Policy
- Suspicious emails must be reported immediately

Personal email accounts may only be accessed outside working hours and must not interfere with duties.

7. Personal Devices

- Personal devices may only be used with Head of School approval
- Devices must be declared and submitted for security checks
- Staff must not contact pupils or parents using personal devices
- Personal devices must be secured with strong passwords
- During lessons, personal devices must be stored away unless required for teaching

If consent for security checks is refused, personal devices must not be used for work.

8. Photography, Video and Recording

- Only school-owned devices may be used to photograph or record pupils
- Appropriate consent must be in place
- Images will only be used for agreed purposes
- Personal devices must never be used to capture images of pupils

9. Removable Media and Cloud Storage

- USB storage devices are not permitted under any circumstances
- Personal or confidential data must not be stored on removable media
- Cloud-based storage must comply with UK GDPR
- Data must not be copied or removed without authorisation

10. Security and Safety

The school will:

- Use firewalls, filtering and malware protection

- Encrypt all devices
- Apply automatic screen-locking
- Restrict software installation to authorised personnel

Staff must:

- Keep passwords confidential
- Report security concerns immediately

11. Loss, Theft and Damage

Staff must take reasonable care of school equipment.
Loss, theft or damage must be reported immediately.

Where damage results from negligence or misuse, the school may seek reasonable and proportionate recovery of costs, considering individual circumstances. Appeals may be made to the Head of School.

12. Unauthorised Use

Staff must not:

- Use ICT for private business or financial gain
- Access or distribute illegal, offensive or discriminatory material
- Install unauthorised software or hardware
- Impersonate others or misuse accounts
- Record images beneath clothing (“upskirting”)

Any breach may result in disciplinary action and, where appropriate, referral to external agencies.

13. Loaning and Purchasing Equipment

- Equipment loans follow the Loaning School Equipment Policy

- Loan requests must be authorised and time-limited
- All equipment remains the property of the school
- Purchases must follow the Finance Policy and be approved in advance

14. Implementation and Compliance

Breaches of this policy may result in:

- Withdrawal of ICT access
- Disciplinary action
- Legal or regulatory action where appropriate

15. Monitoring and Review

This policy will be reviewed every three years or sooner if required due to legislative or operational changes.
Staff will be informed of any amendments.

Loan Request Form

This form should be completed by staff members when requesting to loan school-owned equipment.

Staff members must detail the specific equipment or device which is requested, as well as provide a reason, and where necessary, evidence, as to why the equipment or device is required.

The completed form should be returned to the designated equipment lead (DEL) for authorisation.

Name		**Department**	

Equipment required			
Reason			
First date of loan		**Return date**	
Authorised (if rejected, detail why)			
Signed (CFO)			
Job role		**Date**	