IT Security Policy

Ace London School

1. Policy Statement

Ace London School is committed to protecting the confidentiality, integrity, and availability of all information and communication technology (ICT) systems, data, and resources.

This policy establishes principles and procedures for maintaining a secure digital environment that supports teaching, learning, administration, and compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

The school recognises that information security is essential to maintaining trust, complying with regulatory obligations, and ensuring the continuity of operations.

2. Purpose

The purpose of this policy is to:

- Safeguard school data, IT systems, and digital assets against unauthorised access, loss, or damage
- Ensure compliance with UK GDPR, Data Protection Act 2018, and other relevant legislation
- Define acceptable use of IT systems and responsibilities of staff and students
- Reduce risks of cyberattacks, malware, and data breaches
- Promote good digital hygiene and security awareness across the school

3. Scope

This policy applies to:

- All staff, students, contractors, visitors, and third-party users of Ace London School IT systems
- All equipment and systems, including

- school computers, laptops, and mobile devices
- Email and cloud services
- Wi-Fi and network infrastructure
- Learning management systems (LMS)
- Personal devices used for school business (BYOD)

All forms of data (electronic and digital), including student records, emails, files, and multimedia.

4. Legal and Regulatory Framework

This policy complies with:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Computer Misuse Act 1990**
- **Freedom of Information Act 2000**
- **Communications Act 2003**
- **Copyright, Designs and Patents Act 1988**
- **Cyber Essentials** and **ICO guidance** on data security

5. Key Principles

The school's IT security framework is based on the following principles:

1. **Confidentiality** – Information is only accessible to authorised individuals.
2. **Integrity** – Information is accurate, complete, and safeguarded from unauthorised modification.
3. **Availability** – Systems and data are available to authorised users when required.
4. **Accountability** – All users are responsible for their actions and adherence to security policies.
5. **Resilience** – Systems are designed to recover quickly from disruption or compromise.

6. Responsibilities

Role	Responsibilities

Principal / Senior Management Team	Overall accountability for IT security governance and compliance.
IT Manager / Network Administrator	Implements and monitors IT security controls, updates systems, and responds to incidents.
Data Protection Officer (DPO)	Ensures compliance with data protection and privacy legislation.
All Staff and Students	Use IT systems responsibly, protect credentials, and report security incidents.

7. User Access Control

- Access to school systems will be restricted based on role and necessity ("least privilege principle").
- Each user will be provided with unique login credentials that must not be shared.
- Passwords must:
  - Be at least 12 characters long
  - Contain upper- and lowercase letters, numbers, and symbols
  - Be changed at least every 90 days.
- Multi-factor authentication (MFA) will be enabled for staff email and administrative accounts
- Accounts of staff or students leaving the school will be deactivated within 24 hours

8. Data Protection and Storage

- All personal and confidential data must be stored securely on school-approved systems (e.g., encrypted servers, secure cloud platforms).
- Data must not be stored on unencrypted USB drives or personal devices.
- Regular backups will be performed to ensure data recovery in the event of a failure or attack.
- Staff must comply with the school's Data Retention and Disposal Policy and Data Protection Policy.

9. Use of Email and Internet

- School email accounts must be used for official communication.
- Users must not send or forward spam, phishing, or offensive content.

- Internet usage must comply with UK law and school policies.
- The following activities are strictly prohibited:
    - Accessing or distributing illegal, discriminatory, or inappropriate material
    - Downloading unauthorised software
    - Using school systems for personal business or commercial gain
    - Circumventing network security or restrictions

10. Bring Your Own Device (BYOD)

- Personal devices used for school purposes must have up-to-date antivirus software and password protection.
- Devices must connect only to the secure school Wi-Fi network.
- The school reserves the right to remove access to its systems if a personal device poses a security risk.

11. Network and System Security

- Firewalls, intrusion detection systems, and antivirus software will be maintained on all school networks.
- Software and operating systems must be kept up-to-date with security patches.
- Only authorised IT staff may install or configure hardware and software.
- All external connections (e.g., VPNs, remote access) must be approved and monitored.

12. Cybersecurity Awareness

- All staff and students must complete annual IT security and data protection training.
- Regular awareness campaigns will be conducted on phishing, password security, and safe browsing.
- Simulated phishing exercises may be used for staff development.

13. Incident Reporting and Response

- All IT security incidents (e.g., data breaches, phishing, malware, unauthorised access) must be reported immediately to the IT Manager or Data Protection Officer.

- The school will investigate incidents promptly, mitigate risks, and document the outcome.
- Serious data breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours in line with the Data Breach Procedure.
- Affected individuals will be notified if required by law.

14. Remote Working and Cloud Systems

- Staff accessing school systems remotely must use secure, encrypted connections.
- Cloud storage (e.g., Microsoft OneDrive, Google Workspace) must be approved by the IT Department.
- Sensitive data must never be stored on personal or public cloud accounts.
- Devices used remotely must be logged off or locked when unattended.

15. Physical Security

- Computer rooms, servers, and network equipment must be located in locked, access-controlled areas.
- Only authorised personnel may access IT infrastructure.
- Portable devices (laptops, tablets) must be stored securely when not in use.

16. Software Licensing and Copyright

- All software used by the school must be properly licensed and legally obtained.
- Users must not install or distribute unlicensed or pirated software.
- Breach of software licensing terms may result in disciplinary or legal action.

17. Monitoring and Compliance

- The IT Department may monitor system usage, email traffic, and internet activity for security and compliance purposes.
- Monitoring will be conducted lawfully and proportionately in accordance with the Investigatory Powers Act 2016 and College Privacy Policy.

18. Disciplinary Action

Any breach of this policy may lead to disciplinary action under the Staff Code of Conduct or Student Behaviour and Disciplinary Policy, and in serious cases, legal prosecution under the Computer Misuse Act 1990.

19. Policy Review

- This policy will be reviewed annually by the IT Manager and Data Protection Officer to ensure ongoing compliance and effectiveness.
- Updates will reflect new technological developments, security threats, and legal requirements.

20. Contact Information

IT and Network Security Department

Meerab Majid - Ace London School

Suite 302, 315 & 504 Olympic House

28–42 Clements Road, Ilford, IG1 1BA

meerab@acelondonschool.co.uk