POLICY

IT ACCEPTABLE USE

Approval Date	**November 2025**
Review Date	**2026/27 AUTUMN TERM**
Owner	CFO

Policy Type		
	■	Trust Policy to be adopted in full
		Trust Policy adapted by the School
		School Policy

Approval Body		
	■	Executive
		Trust Board
		Local Advisory Body (LAB)

020 8290 8505
www.orionedu.org.uk
enquiries@orionedu.org.uk

Orion Education
Mansion House, Coopers School
Hawkwood Lane, Chislehurst,
Kent BR7 5PS

Orion Education

Our Four Critical Questions

Why do we exist?

To improve outcomes, transform lives and enable social mobility.

How do we behave?

Trust • Kindness • Endeavour

What do we do?

We create a strong network of schools which transform the lives of students by enabling them to achieve high educational and personal goals, regardless of their background.

How do we succeed?

Through a clear backbone, strong culture, academic rigour and smart systems.

Contents

1. Introduction 3
2. Provision and Use of IT Systems 4
3. Network Access and Security 4
4. Email and Communication 4
5. Internet Access 5
6. Digital Images and File Storage 5
7. Mobile Phones 5
8. Social Networking 5
9. Video Conferencing and Remote Working 5
10. Monitoring of IT Systems 6
11. Artificial Intelligence (AI) Acceptable Use 6
11.1. General Principles 6
11.2. Data Protection and Security 6
11.3. Safeguarding and Risk Management 6
11.4. Transparency and Accountability 6
11.5. Training and Awareness 6
12. Failure to Comply 6
13. Acceptable Use Agreement 7

1. Introduction

This policy enables the acceptable use of IT resources for staff, trustees, governors, and all users within Orion Education. The Trust provides a range of IT resources to support teaching, learning, administration, and safeguarding. To ensure the safety and security of all users—including pupils—it is essential that everyone follows the guidelines set out below.

This policy aims to:

- Promote professional, ethical, lawful, and productive use of Orion Education's IT systems and infrastructure.
- Define and identify unacceptable use of Orion Education IT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why and how monitoring of IT systems may take place.
- Define and identify unacceptable use of social networking sites and Trust devices.
- Specify the consequences of non-compliance.
- Provide guidance on the safe and responsible use of Artificial Intelligence (AI) in education.

This policy applies to all staff, trustees, governors, and users of Orion Education IT systems. All users must read, understand, and sign the Acceptable Use Agreement attached to this policy. Breaches may result in disciplinary action, up to and including dismissal.

2. Provision and Use of IT Systems

- All equipment that constitutes Orion Education's IT systems is the sole property of the Trust. Personal equipment must not be connected to or used with Trust IT systems.
- Users must not install software without permission from Trust IT Support. Unauthorised installations may result in personal liability for any resulting damage.
- IT equipment may be removed for maintenance, reallocation, or operational reasons with 24 hours' notice.
- Users must not make any physical alterations to Trust computer or network hardware.

3. Network Access and Security

- All users must be registered and have a unique network account (username, password, email).
- Passwords must be complex (minimum 8 characters, including capitals, numbers, and symbols) and changed annually.
- Users are responsible for all activities under their account and must not share credentials except with IT Support for system support.
- Any suspected security breach must be reported to IT Support immediately.
- Users must only access authorised areas and must lock or log off computers when unattended.

Pupil use of staff accounts is strictly prohibited unless directly supervised.4. Email and Communication

- School/Trust email is for academic and professional use, with limited personal use during breaks.
- All school-related communication must use the official school email address.
- Sending or receiving offensive, abusive, illegal, or inappropriate content is strictly forbidden.
- Do not use personal email addresses for school business.
- Sensitive or personal information must only be sent using secure, encrypted email or password protection.
- Emails must not contain children's full names; use initials where possible.
- All email use must comply with data protection legislation and other relevant policies.
- Offensive communications must be reported immediately.

5. Internet Access

- Internet access is provided for academic and professional use, with reasonable personal use permitted.
- The Trust's internet connection is filtered, but any inappropriate material accessed must be reported to IT Support.
- Accessing, downloading, or transmitting illegal, offensive, or harmful material is strictly prohibited and may constitute gross misconduct.
- Misuse may result in disciplinary action, including summary dismissal, and may be reported to the police if criminal activity is suspected.

6. Digital Images and File Storage

- Only Trust-provided digital cameras and devices may be used for school purposes.
- Photos for external use must only include a child's first name.
- Personal digital cameras and mobile phones must not be used for taking photos of pupils.
- All school-related work must be stored on OneDrive or approved network drives; personal files are not permitted.
- Use of removable media (e.g., memory sticks) is prohibited unless approved and encrypted.
- No Trust data is to be stored on home computers or unencrypted devices.

7. Mobile Phones

- Mobile phones are permitted but must not be used when supervising or working with children.
- Personal mobile phone cameras are not to be used on school trips.
- All parent contact must be through school phones; personal numbers must not be shared.

8. Social Networking

- Staff must protect the reputation of Orion Education and treat all colleagues and students with professionalism and respect online.
- Use of social networking for school business is only permitted via official channels and with Headteacher approval.
- No school information, documents, or images should be posted on personal social media.
- No details or opinions about pupils or staff are to be published online.
- Cyberbullying or causing distress via social media is strictly prohibited.

9. Video Conferencing and Remote Working

- Only school-approved video conferencing platforms may be used, with school accounts and complex passwords.
- Sensitive material must not be shared over video conferencing platforms.
- Remote working must follow good practice, including securing sensitive data and using only school-approved devices.
- Multi-factor authentication is required for off-site access to Microsoft Office 365 services.

10. Monitoring of IT Systems

- Orion Education may monitor IT system use, including websites accessed, emails, and stored data, to ensure compliance, operational effectiveness, and safeguarding.
- Monitoring is conducted in line with the Data Protection Act 2018 and relevant codes of practice.
- Any inappropriate material found will be deleted, and breaches may be investigated and reported to authorities if necessary.

11. Artificial Intelligence (AI) Acceptable Use

11.1. General Principles

- AI tools can enhance teaching, learning, and administration, but must be used responsibly, ethically, and in line with legal and safeguarding requirements.
- Staff must keep themselves up to date with their own training on the safe and effective use of AI, including understanding its limitations and risks. Staff can seek support from the Trust regarding where to obtain appropriate training. The Trust will provide training on an ad hoc basis; however, due to the fast-paced nature of AI development, staff are expected to proactively maintain their own knowledge and skills.

11.2. Data Protection and Security

- **Sensitive or personal data must never be uploaded to any AI system unless it is an Orion Education-approved, secure platform with appropriate data protection agreements in place.**
- AI-generated content must be fact-checked before use or dissemination.

11.3. Safeguarding and Risk Management

- AI must not be used to access, generate, or disseminate harmful, offensive, or inappropriate content.
- Staff must carry out risk assessments for any new AI tool before use in school.

11.4. Transparency and Accountability

- Any incidents involving AI misuse or data breaches must be reported immediately to the Data Protection Officer.

11.5. Training and Awareness

- The school will keep up to date with DfE and sector guidance on AI and update this policy as required.

12. Failure to Comply

Failure to comply with this policy may result in disciplinary action, including loss of access to IT resources, suspension, or dismissal. Serious breaches may be reported to the police or other authorities.

13. Acceptable Use Agreement

All users must sign the Acceptable Use Agreement confirming they have read, understood, and agree to comply with this policy.

For further information or clarification, please contact the Chief Financial Officer or Data Protection Officer