POLICY

CYBER SECURITY

Approval Date	**November 2025**
Review Date	**2027/28 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 4
2. Purpose and Scope 4
3. Regulatory Alignment 4
4. What is Cyber-Crime? 4
5. Principles 4
6. Roles and Responsibilities 5
7. Technical Controls 5
8. User Controls and Guidance 5
9. Incident Management 6

1. Introduction

Cyber security is a critical risk for the Trust. Every employee, trustee, governor, and student must contribute to data security. The Trust invests in technical cyber security measures, but vigilance and responsible action from all users are essential to protect Trust and School IT systems. The managed service provider is responsible for cyber security within the Trust. Breaches of this policy may result in disciplinary action. This policy supplements other data management and security policies, including the Data Protection Policy, IT Acceptable Use Policies, and Home Working Policy.

2. Purpose and Scope

This policy establishes systems and controls to protect the Trust from cyber criminals and associated risks and sets out an action plan should the Trust fall victim to cyber-crime. It applies to all staff, students, trustees, and governors.

3. Regulatory Alignment

This policy is designed to comply with:

- The Academy Trust Handbook
- RPA (Risk Protection Arrangement) conditions
- National Cyber Security Centre (NCSC) 10 Steps to Cyber Security
- Data Protection Act 2018 and UK GDPR
- Other relevant statutory and regulatory requirements

4. What is Cyber-Crime?

Cyber-crime includes criminal activity using computers or the internet, such as hacking, phishing, malware, viruses, or ransom attacks. Consequences can include financial loss, data breaches, regulatory penalties, reputational damage, business interruption, and organisational instability.

5. Principles

- Cyber security is a shared responsibility across the Trust.
- The Trust Board and Executive Team must maintain oversight and receive regular updates on cyber risks, incidents, and mitigations.
- All staff must receive regular, risk-based cyber security training and participate in simulated phishing campaigns.

- The Trust must maintain a risk-based approach to securing data and systems, including regular risk assessments and asset management.
- Incident response plans must be documented, communicated, and regularly exercised.
- Supplier cyber security must be assessed as part of procurement.
- The Trust must maintain compliance with all relevant regulations and best practices.

6. Roles and Responsibilities

- **CFO:** The CFO is responsible for reporting to the Board and also ensuring an appropriate contract is in place with a managed service provider, who are responsible for all other technical and procedural cybersecurity measures.
- **Managed Service Provider (MSP):** Responsible for the technical implementation of cybersecurity controls, ongoing monitoring of systems, and leading incident response activities. The MSP is the primary responder for any cybersecurity incident, ensuring all technical and procedural measures are in place and effective.
- **All Staff, Trustees, Governors, and Students:** Must comply with this policy, complete training, and report incidents or concerns.

7. Technical Controls

The Trust implements the following technical measures:

- **Firewalls:** Onsite Smoothwall firewalls and ISP-level firewalls in the cloud.
- **Anti-Virus/Anti-Malware:** Centrally managed Trend Micro Security Agent on all Windows devices.
- **Anti-Spam:** Microsoft 365 service.
- **Patching:** Automatic updates for Windows devices; infrastructure hardware patched by RM.
- **URL Filtering:** Smoothwall devices at each site.
- **Secure Data Backup:** Veeam Disk-Disk-Cloud for on-premises; Barracuda for M365; Arbor daily backups.
- **Device Encryption:** Windows Bitlocker for portable devices.
- **Account Management:** Automated provisioning and deprovisioning via SalamanderSoft and Arbor/Active Directory.
- **User Restrictions:** Users cannot install software or disable security features.
- **Password Policy:** Strong passwords (minimum 8 characters, mixed case, numbers, symbols).
- **Multi-Factor Authentication (MFA):** To be implemented for all remote access.
- **Network Segmentation:** Secure, separated wireless access and network infrastructure.
- **Logging and Monitoring:** Datto RMM for monitoring, alerting, and dashboard visibility.
- **Asset Management:** Move towards a centralised asset register for full IT estate visibility.

8. User Controls and Guidance

All users must comply with the IT acceptable use policy.

9. Incident Management

- The Trust maintains a Cyber Incident Response Plan (CIRP), which must be communicated to all relevant staff and regularly exercised through scenario-based drills.
- The CIRP must include discrete playbooks for high-risk scenarios.
- All incidents must be reported promptly to the CFO, who will coordinate response and regulatory notifications as required.
- Where personal data is involved, the Data Protection Policy will be invoked.