Orange Tree School

Orange Tree School Cyber Security Policy 2026–2027

Orange Tree School (Main Site) and Ridgeway Hospital Provision

Policy Summary

Purpose

Orange Tree School is committed to maintaining a secure digital environment that protects pupils, staff, personal data and the continuity of education.

This policy sets out the school's approach to cyber security, including the protection of information systems, devices and digital services from cyber threats, unauthorised access, data loss and disruption.

The policy supports the school's safeguarding responsibilities by ensuring that technology is managed securely, clear reporting arrangements are in place, risks are minimised and cyber incidents are responded to promptly and effectively.

Core Principles

- Cyber security is everyone's responsibility.
- Personal and sensitive information must be protected at all times.
- The school will take reasonable technical and organisational measures to protect its information systems and data.
- Staff will receive appropriate cyber security training and report concerns promptly.
- The school will maintain effective arrangements for preventing, detecting and responding to cyber security incidents.
- Cyber security arrangements will be reviewed regularly to reflect emerging risks, technological developments and statutory guidance.

Key Expectations

- All users will use school systems responsibly and in accordance with the school's acceptable use expectations and relevant policies.
- Strong passwords and multi-factor authentication will be used where appropriate.
- Access to systems and information will be based on business need and reviewed regularly.
- Devices, software and cloud services will be maintained securely and updated appropriately.
- Suspected cyber incidents, phishing emails or data breaches must be reported immediately to the IT Support Officer, with the Business Manager copied into the communication.
- All staff will complete regular cyber security awareness training.
- Third-party suppliers must meet appropriate cyber security and data protection requirements.

Legislation and Guidance

This policy has been developed with reference to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Network and Information Systems Regulations (where applicable)
- Keeping Children Safe in Education (current edition)
- Department for Education Cyber Security Standards for Schools and Colleges
- National Cyber Security Centre (NCSC) guidance
- Education (Independent School Standards) Regulations 2014

DOCUMENT DETAILS	
Applies To:	• All Staff • External suppliers or visitors • Regulatory / Legal bodies/LEAs • Other (e.g. Parents) • Hospital Staff
Policy Author:	Helen Carmel/Zoe Ramshaw
Approval Body:	Advisory Board – Peter Curtis
Frequency of review:	Annually
Last Update:	02/08/2026
Next Review Date:	02/08/2027

Contents

1. Introduction

Orange Tree School is committed to maintaining a safe, secure and resilient digital environment that supports teaching, learning, safeguarding and the effective operation of the school. Digital technologies play an essential role in the education of our pupils, the delivery of therapeutic and pastoral support, communication with families and professionals, and the management of sensitive personal information.

As a specialist independent school for pupils with Education, Health and Care Plans (EHCPs), the school recognises that the availability, integrity and confidentiality of information systems are essential to protecting pupils, supporting staff and maintaining the continuity of education. Effective cyber security helps safeguard personal data, reduces the risk of disruption to learning and ensures that the school can continue to operate safely in the event of a cyber incident.

Orange Tree School adopts a proactive approach to cyber security through appropriate technical controls, secure working practices, staff training and effective incident management. Cyber security is recognised as a shared responsibility, and all members of the school community are expected to contribute to maintaining a secure digital environment.

This policy should be read alongside the School's Online Safety Policy, Data Protection Policy, Mobile Phone and Personal Devices Policy and other related safeguarding and information governance policies.

The school recognises that effective cyber security depends not only on technical controls but also on clear communication, shared responsibility and prompt reporting of concerns.

2. Legal and Regulatory Framework

This policy has been developed with regard to:

- The Education (Independent School Standards) Regulations 2014;
- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Keeping Children Safe in Education (current edition);
- Department for Education Cyber Security Standards for Schools and Colleges;
- National Cyber Security Centre (NCSC) Cyber Security Toolkit for Schools;
- Computer Misuse Act 1990;
- Network and Information Systems Regulations (where applicable);
- ICO guidance relating to personal data security and data breaches.

Orange Tree School recognises that effective cyber security supports the school's safeguarding responsibilities, protects personal information and ensures the continuity of education. The school will review its cyber security arrangements regularly to reflect changes

in technology, emerging threats and statutory guidance and are informed by recognised national guidance and risk assessment.

3. Purpose and Scope

This policy applies to all members of the Orange Tree School community, including employees, volunteers, members of the advisory board, contractors, agency staff, visitors and third-party suppliers who have access to the school's information systems, devices, networks or data.

It applies to:

- desktop computers;
- laptops;
- mobile devices;
- cloud-based systems;
- email services;
- Microsoft 365;
- internet services;
- network infrastructure;
- backup systems;
- removable media;
- any personal data processed on behalf of the school.

This policy should be read alongside the School's Online Safety Policy, Data Protection Policy and Mobile Phone and Personal Devices Policy.

4. Roles and Responsibilities

Advisory Board

Responsible for:

- ensuring appropriate cyber security governance;
- receiving assurance that cyber security risks are managed effectively;
- monitoring significant cyber security incidents where appropriate.

Headteacher

Responsible for:

- ensuring effective cyber security arrangements are in place;
- allocating appropriate resources;
- overseeing strategic cyber security risks;
- ensuring business continuity following any significant cyber incident.

Business Manager

Responsible for:

- overseeing the implementation of this policy;
- line managing the IT Support Officer;
- maintaining operational oversight of all reported cyber security incidents;
- determining the severity of cyber security incidents;
- coordinating the school's response to significant incidents;
- liaising with Netec where specialist technical support is required;
- informing the Headteacher of significant incidents;
- working with the Data Protection Officer where personal data may have been compromised;
- reviewing trends and ensuring lessons learned are implemented.

IT Support

Responsible for:

- providing first-line IT support to staff;
- managing user accounts, passwords and permissions;
- implementing routine security updates and patches;
- monitoring routine cyber security issues;
- receiving and recording all reported cyber security incidents;
- keeping Helen Carmel informed of all reported incidents and escalating concerns where appropriate;
- supporting staff with the secure use of school systems.

External IT Provider (Netec)

Responsible for:

- providing specialist cyber security expertise;
- supporting network infrastructure and security;
- responding to significant technical incidents;
- advising on system resilience and recovery.

Staff should report concerns through the school's internal arrangements and should not normally contact Netec directly.

Data Protection Officer (Aanika Patel)

Responsible for:

- advising on data protection compliance;
- supporting the management of personal data breaches;
- providing specialist advice where cyber incidents affect personal information;
- liaising with the Information Commissioner's Office (ICO) where appropriate.

All Staff

Responsible for:

- following this policy;
- protecting passwords and accounts;
- reporting suspicious emails or cyber security incidents immediately to Craig Hunter (IT Support Officer), copying Helen Carmel (Business Manager) into the communication;
- completing mandatory cyber security training;
- using school systems responsibly;
- protecting confidential information.

5. Technical Security Measures

Orange Tree School implements appropriate technical and organisational measures to reduce cyber security risks and protect the confidentiality, integrity and availability of its information systems.

Cyber security arrangements are proportionate to the size and nature of the school and are reviewed regularly in response to emerging threats and technological developments.

The school's cyber security measures include:

- secure network infrastructure protected by firewalls and appropriate filtering;
- endpoint protection, including anti-virus and anti-malware software on all school-managed devices;
- regular software updates and security patch management;
- secure backup arrangements and tested recovery procedures;
- role-based access controls to systems and sensitive information;
- multi-factor authentication (MFA) where appropriate, particularly for administrative and cloud-based systems;
- secure configuration and monitoring of Microsoft 365, cloud services and remote access;
- encryption of portable devices where appropriate;
- secure disposal of electronic equipment and storage media;
- regular monitoring of network security and system performance; and
- prompt removal or amendment of user accounts when staff leave or change roles.

Technical security arrangements are managed by the IT Support Officer under the direction of the Business Manager, with specialist support provided by Netec where required.

The school's technical security arrangements are reviewed regularly in partnership with the external IT provider to ensure they remain effective and proportionate to emerging cyber risks.

6. User Accounts and Access Control

Access to school systems is provided only where there is a legitimate business or educational need. Access rights are based on individual roles and responsibilities and are reviewed regularly.

Access permissions will be reviewed periodically and whenever a member of staff changes role or leaves the school.

Orange Tree School expects all users to:

- use only their own login credentials;
- maintain strong passwords in accordance with current National Cyber Security Centre guidance and never share authentication credentials;
- never share passwords or authentication codes;
- use multi-factor authentication where provided;
- lock devices when left unattended;
- report suspected unauthorised access immediately;
- use school systems only for authorised purposes.

User accounts will be created, amended and removed by the IT Support Officer as authorised by the Business Manager.

Personally owned devices used to access school systems must comply with the School's Mobile Phone and Personal Devices Policy and any additional security requirements determined by the school.

Artificial Intelligence

Staff using approved AI tools as part of their professional duties must ensure that confidential, safeguarding or personal information is not entered into publicly available AI platforms unless this has been authorised by the school and complies with data protection requirements.

7. Cyber Security Incident Management and Business Continuity

Orange Tree School recognises that timely reporting and effective management of cyber security incidents are essential to protect pupils, staff, sensitive information and the continuity of education. All staff have a responsibility to remain vigilant and to report any actual or suspected cyber security concerns promptly.

Cyber security incidents may include, but are not limited to:

- phishing or suspicious emails;
- malware or ransomware attacks;

- compromised passwords or user accounts;
- unauthorised access to school systems or information;
- loss or theft of school devices;
- accidental disclosure of confidential or personal information;
- disruption to school networks, cloud services or digital systems.

Reporting a Cyber Security Incident

Any member of staff who becomes aware of a suspected cyber security incident must:

- stop using the affected device or system where appropriate;
- preserve any relevant information or evidence;
- report the concern immediately to Craig Hunter (IT Support Officer) and copy Helen Carmel (Business Manager) into the communication;
- report any suspected loss of personal data or confidential information without delay.

Where Craig Hunter is unavailable, staff should report concerns directly to Helen Carmel.

Initial Response

Craig Hunter will provide first-line support by:

- assessing the reported issue;
- taking immediate steps to reduce further risk where appropriate;
- recording the incident;
- keeping Helen Carmel informed of all reported cyber security concerns.

Helen Carmel has overall operational responsibility for cyber security and will oversee the management of all reported incidents. She will:

- determine the seriousness of the incident;
- provide support and direction to the IT Support Officer where required;
- decide whether the incident requires escalation;
- liaise with Netec, the School's external IT support provider, where specialist technical assistance is required;
- inform the Headteacher of any significant cyber security incident;
- liaise with the Data Protection Officer (Aanika Patel) where there is a suspected personal data breach or other data protection concern.

Business Continuity

Where a cyber security incident has the potential to disrupt the operation of the School, Helen Carmel will coordinate the operational response in conjunction with the Headteacher and Netec.

The school maintains appropriate backup, recovery and business continuity arrangements to minimise disruption to:

- teaching and learning;
- safeguarding systems;
- communication with families and professionals;
- access to essential school information.

Learning from Incidents

Following any significant cyber security incident, the school will undertake a review to:

- identify the cause of the incident;
- evaluate the effectiveness of the response;
- identify lessons learned;
- strengthen technical and organisational security measures where necessary;
- provide additional guidance or training to staff where appropriate.

8. Staff Awareness, Training and Reporting

Orange Tree School recognises that staff awareness is one of the most effective ways of reducing cyber security risk.

All staff will receive appropriate cyber security training as part of induction and at regular intervals thereafter.

Training may include:

- recognising phishing emails;
- password security;
- safe use of school systems;
- protecting personal information;
- secure remote working;
- use of cloud services;
- safe use of artificial intelligence;
- reporting cyber incidents;
- current cyber threats and scams.

Staff are expected to:

- remain vigilant;
- follow school procedures;
- seek advice where unsure;
- report concerns promptly.

Staff will also be made aware of the school's internal cyber security reporting arrangements and escalation procedures to ensure concerns are managed promptly and effectively.

Training records will be maintained by the school and reviewed as part of the school's quality assurance arrangements.

9. Monitoring and Review

The Headteacher has overall responsibility for ensuring that this policy is implemented effectively across Orange Tree School.

Day-to-day operational oversight of cyber security arrangements is delegated to the Business Manager, supported by the IT Support and the school's external IT support provider.

The effectiveness of this policy will be monitored through:

- review of cyber security incidents and lessons learned;
- monitoring of system vulnerabilities and technical updates;
- review of staff training and awareness;
- audits of user accounts, access permissions and security controls;
- review of third-party supplier arrangements;
- review of business continuity and backup arrangements;
- recommendations arising from the Data Protection Officer, external IT provider or relevant authorities.

Significant cyber security risks or incidents will be reported to the Headteacher and, where appropriate, the Advisory Board.

Third-party suppliers with access to School systems or information must maintain appropriate cyber security controls appropriate to the services they provide.

Where appropriate, the School will have regard to the Government's Cyber Essentials principles and National Cyber Security Centre guidance when reviewing its cyber security arrangements.

This policy will be reviewed annually, or sooner in response to changes in legislation, statutory guidance, technology or following a significant cyber security incident.

10. Related Policies

This policy should be read alongside:

- Data Protection Policy
- Mobile Phone and Personal Devices Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- CCTV Policy