



# Old Park Primary School & Nursery

## School Cyber Security Policy V2

Model policy: T&W Safeguarding data protection team

**Reviewed:** November 2025

**Next Planned Review:** November 2026

**Definition of Cyber Security:** Application of technologies, processes and controls to protect systems, networks and data from cyber-attacks.

## **Introduction**

The protection of information and communication technologies (ICT) within a school environment is paramount. This Cyber Security Policy aims to establish a framework for maintaining the security and integrity of digital resources, protecting personal data, and ensuring a safe digital environment for students, staff, and stakeholders.

This policy is aligned with the requirements of the Department for Education and National Cyber Security Centre.

## **Scope**

This policy applies to all students, staff, governors and external partners, who have access to school ICT resources.

## **Objectives**

- To protect the confidentiality, integrity, and availability of digital information.
- To safeguard the personal data of students, staff, and stakeholders.
- To ensure compliance with relevant legal and regulatory requirements.
- To foster a culture of cyber security awareness and responsibility.
- To respond effectively to cyber security incidents and breaches.

## **Roles and Responsibilities**

### School Administration

The administration is responsible for:

- Ensuring the development and implementation of the cyber security policy.
- Ensuring adequate resources are allocated for cyber security measures.
- Overseeing cyber security training and awareness programs.
- Reviewing and updating the policy periodically.

### IT Support

IT support is tasked with:

- Maintaining and securing the school's IT infrastructure.
- Implementing technical measures to protect against cyber threats including:
  - Use of anti-malware and firewalls
  - Regular patching and software updates
  - Secure configuration of devices and networks
  - Use of Multi-Factor Authentication (MFA) for staff and privileged accounts
  - Controls over user accounts and access privileges including a review of accounts and prompt removal of leavers
- Monitoring network activity for potential security breaches.
- Responding to and mitigating the effects of cyber security incidents.
- Back-ups are periodically tested with at least one back up kept offline
- Provide web filtering and monitoring of internet access to prevent access to malicious sites

## Staff

All staff members must:

- Adhere to the cyber security policy and procedures.
- Participate in cyber security training and awareness programs.
- Report any suspicious activities or security incidents.
- Safeguard their login password.
- Use MFA where possible

## Students

Students have the responsibility to:

- Follow the school's cyber security guidelines and rules.
- Respect the privacy and security of others.
- Report any cyber security concerns to a teacher or other school staff.

## Acceptable Use Policy

All users of the school's IT resources must adhere to the Information Security Policy, which includes:

- Using school IT resources for educational purposes only.
- Not accessing, sharing, or downloading inappropriate content.
- Respecting intellectual property rights and avoiding plagiarism.
- Not engaging in cyberbullying, harassment, etc.
- Protecting personal information and not sharing login details.

## Data Protection

The school is committed to protecting the personal data it processes. Measures include:

- Where necessary, encrypting sensitive data to prevent unauthorised access.
- Regularly updating software and systems to address vulnerabilities.
- Implementing access controls to restrict data access based on roles.
- Conducting data audits to ensure compliance with data protection laws.

## Cyber Security Training and Awareness

To ensure a culture of security:

- Training sessions will be conducted for staff and students.
- Awareness campaigns on the importance of cyber security will be promoted.
- Resources and materials on best practices will be made available.

## Incident Response

In the event of a cyber security incident:

- The IT department will initiate an immediate investigation.
- Containment measures will be implemented to prevent further damage.
- Affected individuals will be informed promptly.
- A report detailing the incident and response actions will be documented.
- Preventative measures will be revised to avoid future occurrences.

In addition, all incidents and near misses will be reviewed with lessons learnt feeding into policy update and staff training.

## Annual Cyber Risk Assessment

It is best practice to complete an annual Cyber Risk Assessment and undertake termly reviews of this assessment. An assessment should include:

- Identifying and prioritising critical assets
- Identifying threats and vulnerabilities
- Assess the likelihood and impact of each risk
- Evaluate existing controls relating to each risk
- Identify gaps and actions needed to fill these
- Assign responsibilities and timescales for each action
- Document your assessment and review
- Review assessment regularly

A simple example of a cyber risk assessment can be found on **Appendix A**.

## Compliance and Review

Compliance with this policy is mandatory. The policy will be reviewed every 2 years or as required to:

- Ensure it covers evolving cyber security threats and best practices.
- Incorporate feedback from stakeholders.
- Adapt to changes in legal and regulatory requirements.

## Conclusion

Cyber security is a collective responsibility. By adhering to this policy, the school can protect its digital resources, maintain the integrity of personal data, and create a safe and secure environment conducive to learning and growth. Let us all commit to fostering a culture of vigilance and responsibility in our digital interactions.

## Further Reading

NCSC Cyber Essentials Framework - [Cyber Essentials - NCSC.GOV.UK](#)

NCSC Cyber Security for schools - [Cyber Security for Schools - NCSC.GOV.UK](#)

DfE Cyber Security Standards - [Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK](#)

LGfL Elevate Cyber Security Toolkit - [Elevate Cyber Security Toolkit | LGfL](#)

Example of a cyber security assessment

Asset	Threat	Vulnerability	Likelihood	Impact	Existing Controls	Action Needed	Deadline
<i>Staff email</i>	<i>Phishing</i>	<i>Lack of training</i>	<i>Medium</i>	<i>High</i>	<i>MFA</i>	<i>More training</i>	<i>Autumn term</i>