

OAKTREE PRIMARY SCHOOL

An Athena Education School

CYBER SECURITY AND E-SAFETY POLICY

Developing Confident, Safe and Responsible Digital Citizens

Policy Title	Cyber Security and E-Safety Policy
Institution	Oaktree Primary School
Operator	Athena Education
Applies To	All staff, pupils, governors and contributors to teaching, learning and operations
Version	1.0
Academic Year	2026/27
Status	Approved
Approved By	Director of Schools / Principal / SGAB
Date of Approval	25 June 2026
Last Reviewed	20 August 2026
Next Review Date	20 August 2027
Policy Owner	Principal / IT Team
School Leader Signature	

Contents

1. Policy Statement	3
2. Purpose	3
3. Scope	3
4. Roles and Responsibilities	3
5. Acceptable Use of Technology	3
6. Passwords & Device Security	4
7. Internet, Email & Social Media	4
8. E-Safety Education (Primary Focus)	4
9. Monitoring and Incident Management	4
10. Disciplinary Measures	4

1. Policy Statement

Oaktree Primary School recognises that technology is a powerful tool for learning. At the same time, it presents risks if not used responsibly. This policy ensures that pupils and staff are protected when using digital resources and that our school meets the highest standards of online safety and cybersecurity.

2. Purpose

This policy exists to:

- Pupils must not be exposed to harmful images, inappropriate websites, or unsafe contact with strangers.
- Personal details, attendance data, and assessment results must always be kept secure and confidential.
- Everyone must understand that technology should be used positively and respectfully.
- The school follows the UAE Cybercrime Law, Child Rights Law, and Dubai Data Law to ensure all digital activity is lawful.

3. Scope

This policy covers:

- Pupils, staff, governors, parents, volunteers, and visitors are expected to follow these rules.
- This includes school-owned laptops and tablets, BYOD devices, Wi-Fi use, and online learning platforms such as Google Workspace and Seesaw.

4. Roles and Responsibilities

- The Principal and SLT should make sure this policy is enforced and reviewed regularly. They ensure resources are available to support safe practice.
- DSL (Safeguarding Leads) keeps records of incidents, delivers staff training, and contacts outside agencies when required.
- IT Department maintains secure networks, updates antivirus software, and manages firewalls. Responds quickly to threats and ensures systems are working safely.
- Staff must teach and model safe online behaviour. They should only use official school systems for communication and report any issues immediately.
- Pupils are expected to follow classroom e-safety rules. They must report anything suspicious or upsetting online and show kindness in digital interactions.
- Parents should monitor their child's device use at home. They should support the school by encouraging responsible online behaviour.

5. Acceptable Use of Technology

- Devices and networks are for learning or schoolwork, not for gaming, social chatting, or downloading unauthorised content.
- No user may try to access or share websites that contain violence, inappropriate language, or illegal material.
- Staff and pupils must not copy text, images, or videos without giving proper credit to the source.

- Passwords must never be shared with others, including friends or family.
- Pupils and staff must use polite language and avoid any behaviour that could be seen as bullying or harassment.

6. Passwords & Device Security

- Passwords should be at least 8 characters and include numbers, symbols, and both upper- and lower-case letters.
- Passwords must be changed every 90 days to reduce the risk of hacking.
- Any personal device brought to school must be registered with the IT team and checked for antivirus software.
- Pupils and staff must never turn off or change school security settings.

7. Internet, Email & Social Media

- All communication must go through official OPS email addresses and platforms. Personal accounts should not be used.
- Sending rude, offensive, or threatening emails is not allowed. Group emails should be used only for school purposes.
- Pupils are not permitted to use social media during school hours unless supervised for learning purposes.
- Parents must give permission before photographs or videos of children are published on school platforms

8. E-Safety Education (Primary Focus)

- Pupils are taught about safe passwords, spotting fake news, and what to do if they feel unsafe online in assemblies, ICT and PSHE lessons.
- Teachers show pupils how to check information online and explain why not everything on the internet is true.
- Pupils are taught to question information from AI tools, protect their personal data, and use these tools responsibly.
- The school will run workshops and share newsletters so families can reinforce safe practices at home.

9. Monitoring and Incident Management

- The IT team monitors web traffic, blocks unsafe sites, and checks logs regularly.
- Any suspicious email, harmful content, or unusual computer activity must be reported straight away to IT or the DSL.
- Serious cases, such as cyberbullying or hacking, may be referred to KHDA or UAE authorities

10. Disciplinary Measures

- Pupils or staff may lose access to Wi-Fi or devices if they break the rules.
- Pupils may face detention, written warnings, or exclusion depending on the seriousness of the case.
- Misuse by staff may result in formal disciplinary action, up to dismissal.

-
- If laws are broken, the school will report the matter to the appropriate authorities in the UAE.
 - Behaviour Policy followed.