CYBERSECURITY AND DIGITAL SAFETY POLICY

POLICY APPROVED: June 2026

LAST REVIEWED: June 2026

NEXT REVIEW DATE: June 2027

VERSION: 1.0

ACADEMIC YEAR: 2026-2027

PERSON RESPONSIBLE: Mr Andreas Nestorides (Operations Manager)

Contents

Cybersecurity and Digital Safety Policy

For Students, Teachers and Administrative Staff

1 Purpose

The purpose of this policy is to help all members of The Grammar School Nicosia community understand how to protect school electronic systems, personal data and digital resources from cyber threats.

Cybersecurity is the responsibility of everyone who uses school technology systems, including students, teachers and administrative staff.

This policy provides guidance on:

- preventing cyber threats;
- detecting suspicious activity;
- protecting devices, accounts and information;
- responding correctly to cyber incidents;
- using school systems and digital platforms safely and responsibly.

This policy should be read together with the School's Code of Conduct, Discipline Policy, Email Policy, Data Protection Policy, Student iPad Usage Policy, Student Mobile Phone Policy, Smart Devices Usage Policy, Usage of Artificial Intelligence (AI) Policy, Anti-Bullying Policy and Safeguarding and Child Protection Policy, where relevant.

Where a specific student, staff, device or digital-use policy also applies, that policy must be followed together with this Cybersecurity and Digital Safety Policy.

---

2 Preventing Cyber Threats

2.1 Strong Passwords

All users must create strong and secure passwords for school accounts and digital platforms.

A strong password should:

- Be long (at least 12 characters long) and difficult to guess
- Contain a mix of uppercase and lowercase letters, numbers, and symbols

- Be different for each platform or account
- Change periodically, but not longer than 6 months

One effective method is to create a password based on a phrase or sentence that is easy to remember but difficult for others to guess

Example process:

1. Choose a memorable phrase
   Example: *Tommy used to work on the docks*
2. Remove spaces
   Tommyusedtoworkonthedocks
3. Add uppercase letters
   TommyUsedtoworkontheDocks
4. Replace letters with numbers. For example:
   - O/o → 0
   - L/l → 1
   - I/i → 1
   - Z/x → 2
   - E/e → 3
   - S/s → 5

Example: T0mmyU5edt0W0rk0ntheD0ck5

5. Add special characters or replace letters with special characters. For example:
   - A/a → @
   - S/s → $
   - I/i → !

Example: T0mmyU$edt0W0rk0ntheD0ck$!

2.2 Password Rules

Users must also follow these guidelines:

- Do not use personal information such as birthdays, family names, pets, or addresses
- Never share passwords with anyone, including classmates or colleagues
- Use a different password for each system or website
- Do not write passwords on paper or store them in easily accessible places

- Avoid saving passwords on shared devices or browsers
- Avoid common or repeated patterns or words. Examples to avoid: "123456", "111111", "abcdef", "password", simple keyboard sequences like "qwerty"

2.3 Password Resets

Passwords must be changed immediately if:

- a user suspects that their account has been compromised;
- a password has been accidentally shared;
- the user has clicked on a suspicious link or attachment;
- the password has been exposed or forgotten;
- the IT Department instructs the user to change it.

Any difficulty with school account access must be reported to the IT Department or the responsible member of staff.

2.4 Multi-Factor Authentication (MFA)

Where available, users must enable Multi-Factor Authentication, also known as MFA, for school accounts and digital platforms.

MFA provides an extra layer of security by requiring users to verify their identity using a second method, such as:

- a mobile authentication application;
- an SMS verification code;
- email verification;
- another approved verification method.

MFA helps reduce the risk of unauthorised access, even if a password has been compromised.

3 Detecting Cyber Threats

3.1 Phishing, Pharming and Smishing

Users must be alert to common cyber threats, including phishing, pharming and smishing.

Phishing is a fraudulent email designed to trick users into revealing information or clicking unsafe links.

Pharming redirects users to fake websites that look legitimate in order to steal personal, financial or login information.

Smishing is a similar type of attack sent through text messages or SMS.

These attacks may try to persuade users to share:

- passwords;
- personal information;
- financial information;
- school information;
- login details;
- confidential documents or data.

3.2 Warning Signs of Phishing

Users should be cautious if a message:

- comes from an email address that looks unusual or suspicious;
- appears to come from a real organisation but uses a free email service;
- contains unexpected attachments;
- contains spelling or grammar mistakes;
- creates urgency, pressure or fear;
- asks for personal, financial or confidential information;
- asks the user to click on a suspicious link;
- asks for passwords or verification codes;
- makes an unusual request, especially about money, accounts or sensitive information.

Artificial Intelligence tools can make phishing messages look more convincing, so users should not rely only on spelling or grammar mistakes to identify suspicious messages.

3.3 What to Do if You Suspect Phishing

If a user suspects phishing, they must:

- not click on any links;
- not open attachments;

- not reply to the message;
- not share any personal or confidential information;
- check the sender's actual email address carefully;
- report the message immediately to the IT Department or responsible member of staff.

3.4 Warning Signs of Pharming

Users should be cautious if:

- a familiar website looks different or unusual;
- a website asks for information it does not normally request;
- the browser shows a warning about an unsafe or invalid certificate;
- a website behaves strangely;
- files or attachments try to download automatically;
- links do not work correctly or redirect to unexpected pages.

Secure websites usually begin with "https://" and show a padlock icon. However, users should still remain careful, as some fake websites may also appear secure.

3.5 What to Do if You Suspect Pharming

If a user suspects pharming, they must:

- leave the suspicious website immediately;
- not click on any links;
- not enter any personal, financial or confidential information;
- report the concern immediately to the IT Department or responsible member of staff.

---

4 Malware and Unsafe Files

Malware is malicious software designed to damage devices, steal information or gain unauthorised access to systems.

Examples of malware include:

- viruses;
- ransomware;
- spyware;

- Trojan software.

Malware can spread through:

- infected email attachments;
- unsafe downloads;
- suspicious websites;
- unknown programs or browser extensions;
- external storage devices, such as USB drives.

Users must avoid downloading, opening or installing files from unknown or untrusted sources.

If antivirus or security software identifies a suspicious file, users must not open it. They should follow the security software instructions and report the matter to the IT Department where necessary.

---

5 AI-Generated Threats and Deepfakes

Cybercriminals may use Artificial Intelligence to create convincing fake emails, messages, images, videos or voice recordings. These may be used to impersonate trusted individuals or organisations.

Users should:

- verify unusual requests through official communication channels;
- be cautious of urgent requests involving money, passwords, accounts or sensitive information;
- avoid trusting audio, video or images without checking their source;
- report suspicious AI-generated content to the IT Department or responsible member of staff.

Use of AI tools is also covered in the School's Usage of Artificial Intelligence (AI) Policy.

---

6 Protection of Personal Data

All users must handle personal, student, parent and staff information responsibly and in accordance with GDPR, school data protection requirements and the School's Data Protection Policy.

Users must:

- only access information that is necessary for their role or schoolwork;
- avoid sharing confidential information without authorisation;
- store sensitive information securely;
- report any suspected data breach immediately;
- avoid entering personal, private or confidential information into unsafe platforms or tools.

Personal data may include:

- student records;
- parent or guardian contact information;
- assessment data;
- medical or wellbeing information;
- safeguarding information;
- staff records;
- login details;
- personal identification information.

Any suspected loss, exposure or unauthorised sharing of personal data must be reported immediately to the appropriate member of staff, the IT Department, or the person responsible for data protection.

---

7 Mobile Devices, Tablets and Personal Devices

Users who access school systems from mobile devices, tablets or personal devices must take reasonable steps to protect these devices.

Devices used to access school systems should:

- be protected with a password, PIN or biometric authentication;
- be kept up to date;
- use antivirus or anti-malware protection where applicable;
- be locked when not in use;
- not be shared with unauthorised users;

- be reported immediately if lost or stolen and connected to school accounts.

Users should avoid accessing sensitive school systems through unsecured public Wi-Fi networks.

Student use of iPads, mobile phones and smart devices is also governed by the Student iPad Usage Policy, Student Mobile Phone Policy and Smart Devices Usage Policy.

---

8 External Storage Devices

External storage devices, such as USB drives, may present cybersecurity risks.

Users should:

- avoid connecting unknown USB devices to school computers;
- scan removable media for malware before use, where possible;
- use approved storage devices where required;
- avoid transferring confidential or sensitive information through unsecured external devices.

Unauthorised or suspicious external devices must not be connected to school systems.

---

9 Protecting Devices and Information

All users must take basic steps to protect the devices, accounts and systems they use.

9.1 Antivirus and Anti-Malware Protection

Devices should have reliable antivirus or anti-malware protection installed and updated, where applicable.

9.2 Regular Updates

Operating systems, applications and browsers must be kept up to date. Updates often include important security patches that protect devices from known risks.

Automatic updates are recommended where appropriate.

9.3 Safe Software Installation

Users should:

- only download software from trusted and verified sources;

- avoid installing unknown programs;
- avoid installing unnecessary browser extensions;
- not attempt to bypass school security settings.

9.4 Regular Backups

Important files should be backed up regularly to reduce the risk of data loss in case of a cyberattack, accidental deletion, device failure or technical issue.

---

10 Responsible Digital Behaviour

All members of the school community must use digital technologies responsibly, respectfully and safely.

Misuse of school systems, digital platforms, personal devices or online tools may result in action in line with the relevant school policies, including the Code of Conduct, Discipline Policy, Anti-Bullying Policy, Email Policy, Student Mobile Phone Policy, Student iPad Usage Policy, Smart Devices Usage Policy and Usage of Artificial Intelligence (AI) Policy.

This includes, but is not limited to:

- cyberbullying or online harassment;
- unauthorised access to another person's account or device;
- sharing confidential school information without permission;
- sending harmful, offensive or inappropriate content;
- attempting to damage, bypass or interfere with school systems;
- using digital tools in a way that affects the safety, dignity, privacy or wellbeing of others.

---

11 Responding to Cyber Incidents

If a user suspects a cybersecurity issue, or believes that a device, account or system has been compromised, they must act immediately.

Step 1: Report the Issue

The user must inform the IT Department or responsible member of staff immediately.

The IT Department may temporarily suspend or restrict access to the affected account where necessary to protect school systems, personal data and digital resources.

Step 2: Disconnect from the Network

If it is safe and possible to do so, the user should:

- disconnect from Wi-Fi or the school network;
- stop using the affected account or device;
- shut down the affected device if instructed or if the device appears to be unsafe.

Step 3: Do Not Attempt Repairs Yourself

Users must not attempt to remove malware, change system settings, delete evidence or repair the issue themselves unless instructed by the IT Department.

Step 4: Follow IT Instructions

The IT Department will assess the issue and provide instructions on how to proceed.

Users must cooperate with the IT Department and provide accurate information about what happened, including:

- when the issue occurred;
- what device or account was affected;
- whether any links or attachments were opened;
- whether any password or personal information was shared;
- any messages, screenshots or evidence connected to the issue.

---

12 Responsibility of Users

All students, teachers and administrative staff are responsible for:

- protecting their accounts and passwords;
- using school technology responsibly;
- keeping devices secure;
- reporting suspicious activity immediately;
- following the guidelines in this policy;
- cooperating with the IT Department during investigations or security checks.

Failure to follow this policy may result in action in line with the relevant school policies and, where necessary, further action required by law.

13 Policy Review

This policy will be reviewed regularly to ensure that it remains effective, clear and aligned with school procedures, technological developments, cybersecurity risks and relevant legal requirements.

The school may update this policy earlier if required by cybersecurity needs, data protection requirements, safeguarding concerns, changes in technology or school procedures.