DE LA SALLE COLLEGE

LAPTOP POLICY

2025

1. Purpose of the Policy

This policy establishes the expectations and responsibilities for the appropriate use of the students' laptops at De La Salle College. It ensures that all devices and access to the College network are used safely, responsibly, and exclusively for educational purposes that support teaching and learning. The policy safeguards students and staff from exposure to harmful, illegal, or inappropriate online content and cyber risks, while also protecting the integrity of the school's digital infrastructure. By providing clear standards of conduct, supervision requirements, and consequences for misuse, this policy promotes a secure and productive digital learning environment where students can develop essential digital skills in a respectful and ethical manner.

2. Scope

This policy applies whenever the device is being used, both at school and at home. By using the laptop, students agree to follow the guidelines in this policy and use the device responsibly at all times.

3. Roles and Responsibilities

3.1 Students

Students must:

- Use laptops only for school-related learning during and outside school hours.
- Ensure that the device is fully charged before bringing it to school. **Bringing an uncharged device will result in an infraction**.
- Log in using school accounts only.
- Keep passwords private and secure.
- Lock screens when stepping away.
- Report any damage caused by others, concerns, cyberbullying, or suspicious behaviour immediately to a staff member.

- Store the device securely in lockers during breaks and when not in use. Laptops must be carried in the appropriate protective bag when moving between lessons. **Students will be held responsible for any resulting damage if this requirement is not followed**.
- Handle laptops responsibly and avoid damage, stickers, or tampering.
- Label chargers and protective bags to prevent mix-ups.
- Use only authorised Wi-Fi networks.

Students must not:

- Delete or bypass system security tools, download or install unauthorised applications/software, or attempt to hack, bypass filters, or disable monitoring tools. **Such actions will lead to suspension**.
- Share inappropriate media or store non-school material on USB devices. **Any breach of this rule will result in confiscation of the device and may lead to suspension**.
- Record audio or video without permission. **Any breach of this rule will result in a detention or suspension, and any recordings will be permanently deleted**.
- Access, view, share, or store:
    - Pornographic, violent, extremist, or hate-based content.
    - Drug-related or gambling content.
    - Content promoting self-harm or reckless behaviour.
    - Illegal platforms or criminal digital activities.

  Such actions will lead to immediate suspension and may be referred to the relevant authorities.
- Engage in cyberbullying, harassment, or any unauthorised recording of others. **Any breach of this rule will result in detention and a formal meeting with parents/guardians**.

3.2 Teachers

Teachers are expected to:

- Monitor student laptop use during lessons.
- Disable microphones and Microsoft Teams functions when not required for the lesson.
- Address misuse promptly and escalate to SMT when necessary.

3.3 Parents/Guardians

Parents/guardians are expected to:

- Support responsible device use at home.
- Help ensure safe storage and care of the device.
- Report any damage or technical issues occurring outside school hours by contacting the MITA Service Call Centre on 2093 5000.

4. Acceptable Use

Laptops may be used for:

- Classwork, homework, assessments and extended learning.
- Safe and responsible research for school projects.
- Communication with teachers through approved platforms.
- Access to school-managed systems and content.

5. Internet Filtering and Monitoring

To ensure a safe and secure digital environment, all school network and device usage is subject to monitoring and filtering measures.

5.1 Monitoring

All online activity on school devices and networks is logged and monitored. Monitoring tools are used to:

- Detect and prevent access to harmful, illegal, or inappropriate content.
- Safeguard student wellbeing and safety.
- Maintain academic integrity and responsible technology use.

5.2 Filtering

Automated filtering systems restrict access to prohibited categories of online content. Any attempt to bypass or disable these measures is strictly prohibited.

5.3 Restricted/Teacher-Approved Access Only

The following categories may only be accessed **with staff approval and for educational purposes**:

- Video streaming platforms (e.g., YouTube).
- Online games and chat forums.
- AI tools, such as ChatGPT.

5.4 Content Prohibited and Always Blocked

The following categories are permanently restricted:

- Adult content and sexually explicit material.
- Extremist, terrorist, or hate-based content.
- Malware, phishing sites, and hacking tools.
- Social media platforms and unauthorised messaging applications.
- Gambling websites and illegal file-sharing or downloads.
- Drug-related, criminal, or otherwise harmful behaviour content.

5.5 Allowed Content

Approved educational websites and learning tools. Any accidental exposure to harmful content must be reported immediately to a member of staff.

5.6 Enforcement

Any violation of this policy will result in disciplinary action in accordance with the school's Behaviour Policy and Acceptable Use Agreement.

6. Device Use During Non-Lesson Time

To minimise safeguarding risks and protect devices from accidental damage, the following rules apply outside formal lesson time:

- **Break times:** Laptops must remain switched off or closed and stored securely in lockers.
- **Lesson transitions:** Devices must remain closed and must not be used.
- **Study periods/Free lessons:** Laptops may only be used for approved educational tasks and must be under teacher supervision.

Any misuse of devices during unsupervised periods will result in a detention.

7. Security Rules

- Antivirus and system updates must always remain active.
- Students must not tamper with system settings or remove security software.
- Only the official charger may be used.
- USB drives are permitted only with teacher approval.
- Devices must not connect to unauthorised networks.
- Suspicious pop-ups or malware warnings must be reported immediately to the IT administrator.

8. Monitoring and Privacy

The school reserves the right to:

- Review browsing history and online behaviour.
- Inspect installed applications and stored files.
- Monitor communication through school accounts.
- Remotely lock or disable devices if needed.

Students **must not expect privacy** when using school systems. Monitoring exists to protect students, ensure compliance and maintain a safe digital environment.

9. Device Support, Insurance and Loss Claims

(Aligned with MEYR and MITA requirements)

- Devices include a three-year extended warranty.
- Government acts as insurer after warranty expiry (excluding negligence).
- Lost or stolen devices require:
  - Immediate MITA notification, and
  - A valid police report.
- Students leaving Malta must return the device.
- Unreturned devices will be **remotely blocked** and recovered via legal action.

10. Frequently Asked Questions

- *Will replacement devices be provided?*
  No. Replacement devices are not issued by schools. Repaired devices remain on-site until collected by contractor staff.

- *What if damage happens during holidays?*
  Parents/guardians must contact the MITA Service Call Centre on 2093 5000 for guidance.

- *What if damage is due to negligence?*
  Cases of negligent or intentional damage may be referred to an arbitration board set up by **MEYR**.

- *What if a student transfers to another school in Malta?*
  The student must take the device with them. Inventory must be updated and a new AUP signed.

11. Summary of Consequences for Misuse

Type of Misuse	Consequence
Failure to bring a charged device	Infraction recorded
Hacking, bypassing filters, disabling monitoring tools, installing unauthorised software	Suspension
Sharing or storing non-school material on USBs	USB confiscation and possible suspension
Recording audio or video without permission	Detention or suspension + recordings permanently deleted
Accessing harmful or illegal content	Immediate suspension and possible referral to authorities
Cyberbullying/harassment	Detention + mandatory parent/guardian meeting
Unsupervised misuse during non-lesson time	Detention

12. Policy Review

This policy will be reviewed annually by the Senior Leadership Team to ensure continued safeguarding compliance, alignment with cybersecurity standards, and responsiveness to changes in teaching and learning approaches.