



Policy Title	IT Acceptable Use Policy				
Author	AM Redfern				
Date of First Issue	March 2020				
Date of Amendments	AM Redfern Mar 2020	T van Emmenis Nov 2024	T van Emmenis Sep 2026		
Date of Approval SMT	Sep 2020				

IT ACCEPTABLE USE POLICY

1. PREAMBLE, PURPOSE & STATUTORY LEGAL FRAMEWORK

Stanford Lake College is dependent on its technology resources and the information that is accessed via those resources. Much of that information is provided by means of our School Data Network and the internet itself. While these networks, local and worldwide, offer invaluable opportunities for sharing information and for working more efficiently, they also present potential vulnerabilities regarding school data, email accounts, and confidential information. All members of the school community share a responsibility to operate our systems in a way that minimizes vulnerability to our learning, teaching, and administrative work.

Operating as an independent boarding school in Limpopo, Stanford Lake College exercises a strict duty of care (*in loco parentis*) to protect the physical, emotional, and digital safety, privacy, and dignity of all learners, staff, and visitors.

This policy is formulated in accordance with the Constitution of the Republic of South Africa and key statutory frameworks governing child protection, data privacy, and digital communications:

1. **The Constitution of the Republic of South Africa (Act 108 of 1996):** Balances Section 14 (*Right to Privacy*) with Section 28(2) (*The Best Interests of the Child as paramount in every matter concerning the child*).
2. **Protection of Personal Information Act (POPIA) (Act 4 of 2013) – Sections 34 & 35:** Regulates the processing of "Special Personal Information," which explicitly includes photographs, video recordings, audio clips, and personal identifiable data of children. Minors under 18 lack full legal capacity to authorize the public processing or dissemination of their personal data and images; express, written parental/guardian consent is mandatory.
3. **The Children's Act (Act 38 of 2005) & Child Justice Act (Act 75 of 2008):** Mandates child safeguarding against digital exploitation and cyber-grooming. Establishes that minors from age 10 possess legal capacity to be held criminally and civilly liable for harmful digital actions.
4. **Cybercrimes Act (Act 19 of 2020) & Protection from Harassment Act (Act 17 of 2011):** Criminalizes non-consensual sharing of intimate images, harmful or threatening digital messages, intimidation, cyberbullying, extortion, and identity theft.
5. **Films and Publications Amendment Act (Act 11 of 2019):** Prohibits the creation, possession, or distribution of Child Sexual Abuse Material (CSAM), sexualized media involving minors, or cyber-grooming content.





6. **Common Law of Defamation & Contractual Code of Conduct:** Protects the reputation, dignity (*dignitas*), and brand of the school, its staff, and its learners against libel, slander, and public disrepute.

2. SCOPE, RATIONALE & MANDATORY COMPLIANCE

This Acceptable Use Policy covers the use of any computer, electronic device, network infrastructure, or digital facility while on campus, connected to the school's network (wired, Wi-Fi, or cellular), or accessing school systems remotely. This includes IT equipment provided by Stanford Lake College as well as personal devices brought onto campus by students, staff, parents, or visitors (Bring Your Own Device - BYOD).

MANDATORY COMPLIANCE NOTICE:

Compliance with this policy is **compulsory**. Any breach, contravention, or non-compliance by any individual bound by this policy will be treated as serious misconduct and **will attract formal disciplinary action, up to and including dismissal (for staff), expulsion (for learners), cancellation of enrollment contracts (for parents), and potential legal or criminal prosecution.**

This policy must be read in direct conjunction with:

- *Annexure K – Personal Mobile Device Policy*
- *Social Media Policy*
- *Staff Code of Conduct & Disciplinary Code*
- *Learner Code of Conduct & Disciplinary Policy*
- *Parent Contract & Conditions of Enrollment*

3. DEFINITIONS

For the purpose of this document, the following definitions apply:

- **Electronic Devices:** Any electronic data storage, receiver, transmitter, or similar device, including but not limited to cellular phones, personal digital assistants (PDAs), digital cameras, calculators, smartwatches, laptops/notebooks, tablets, audio/video recorders, and portable audio/video players.
- **Internet / Network Access / Connectivity:** Any connection to the internet, intranet, or any other network (external or internal) by any software or application on an electronic device. This includes web browsing, email, peer-to-peer networks, chat services (including WhatsApp), social media platforms, video streaming, Voice-over-IP (VOIP), Bluetooth- or Wi-Fi-based networks, and cellular data connections (e.g., 3G/4G/5G).
- **User:** Any student, employee, service provider, parent, guardian, or visitor who has permission to access the Stanford Lake College network or who brings an electronic device onto school grounds.





- **Student / Pupil:** A registered learner at Stanford Lake College.
- **DoS Attack (Denial-of-Service):** A cyber-attack in which a server, machine, or network resource is made unavailable by disrupting services (including "mail bombing"—sending massive numbers of emails to overwhelm a server or account).
- **Spamming:** The sending of unsolicited, bulk, or harmful electronic communications.
- **Network Drive / Server Storage:** Storage space provided to each user linked to their school account (e.g., H Drive, Resource Drive, Google Drive). Users must have no expectation of absolute privacy on network drives, as the school reserves the right to inspect stored content for unacceptable or illegal material.

4. APPROVED STAFF-LEARNER DIGITAL COMMUNICATION PROTOCOLS

To align directly with *Annexure K* and the *Social Media Policy*, eliminate boundary erosion, and safeguard staff and learners against unmonitored digital contact, the school enforces a single approved digital communication ecosystem.

4.1 Approved Communication Channels

- **Exclusive Channels:** All official digital interaction between staff (teachers, Housemasters/Mistresses, coaches, administrative staff) and learners must take place exclusively through official school-issued Google Workspace accounts via:
 1. **Google Email (Gmail)**
 2. **Google Chat**
- **Audit Trail & Monitoring:** All Google Workspace accounts are centrally managed, archived, and monitored under **Google Vault** and are subject to compliance audits by the Senior Management Team (SMT).
- **Communication Hours:** Non-emergency staff-learner digital communication must occur between **07:00 and 17:30** on school days. Outside these hours, contact must be established via the official House Duty Phone or school landline.

4.2 Prohibited Communication Channels

- **Zero-Tolerance Messaging:** Direct messaging, group chats, or personal social media interactions between staff and learners on WhatsApp, Telegram, Signal, SMS, personal phone calls, Instagram, TikTok, Facebook, Snapchat, Discord, or X are strictly prohibited.
- **Personal Contact Details:** Staff and learners are forbidden from exchanging personal cell phone numbers, personal email addresses, or personal social media handles.
- **Friending/Following Restrictions:** Staff members must not accept current pupils (of any age) or ex-pupils under the age of 18 as friends, followers, or connections on any personal social media account.





5. PERSONAL ELECTRONIC DEVICES (BYOD) & CAMPUS REGULATIONS

Stanford Lake College permits students to be in possession of appropriate electronic devices during school hours or school functions strictly subject to the rules below and in *Annexure K*:

5.1 General Campus Regulations & Storage

- **Liability Disclaimer:** Stanford Lake College accepts no responsibility for the loss, theft, or damage of personal electronic devices under any circumstances. Users are entirely responsible for securing their property. Unattended devices found in public spaces or unlocked boarding house rooms will be confiscated immediately.
- **Day Scholars (Grades 8–12):** Day scholars may bring mobile devices to school, but devices must be **switched off** prior to entering school grounds and handed directly to the Head of Day Scholars before the start of the academic day. Devices will be stored in a locked safe and returned at the end of the academic day.
- **Boarders (Grades 8–10):** Boarders must surrender their devices to duty Boarding Masters/Mistresses outside designated release windows as stipulated in *Annexure K*.
- **Senior Boarders (Grades 11–12):** Senior boarders are permitted controlled device usage for academic preparation, subject to Housemaster/Mistress oversight and boarding house lights-out regulations.
- **Co-Curricular & Inter-School Events:** Grade 8 and 9 learners participating in off-campus co-curricular events must obtain an approved permission slip from their Housemaster/Mistress or Duty Tutor after breakfast to collect their phone.
- **Headphone Restrictions:** Mobile devices may not be used with headphones or earphones in any public spaces on campus.
- **Assembly, Shows & Dining Hall:** Device usage during Assembly, formal shows, inside the Dining Room, or after lights out will result in immediate device confiscation for a period of **ONE WEEK**.

6. ACADEMIC & EXAMINATION RULES

1. **Classroom Rules:** Devices may only be brought into or used in classrooms with express prior authorization from the subject teacher for specific academic activities. Using devices for non-academic purposes during class will result in immediate detention; repeated infractions will result in confiscation.
2. **Examinations & Cycle Tests:** Mobile devices, smartwatches, connected electronic wearables, and unauthorized computing devices are strictly forbidden in examination rooms and cycle test venues.
3. **Academic Dishonesty (Cheating):** Any pupil found in possession of an electronic device or smartwatch during a test or examination—even inadvertently—will be found guilty of cheating and dealt with under the school's Cheating Policy and Disciplinary Code.





7. POPIA COMPLIANCE, MEDIA RIGHTS & INVASIVE RECORDING BAN

1. **Mandatory Parental Consent:** In accordance with POPIA, minors under 18 cannot legally authorize the public publication or processing of their images or personal data. No photographs, video footage, or audio recordings of any learner may be taken, uploaded, or shared on social media or digital platforms without prior express written consent from a parent or legal guardian.
2. **Staff Privacy Rights:** No learner, parent, or visitor may photograph, record, or film any member of staff without their explicit verbal and written permission.
3. **Invasive Recording Ban:** Taking photographs, video footage, or audio recordings in private or sensitive spaces—including boarding house bedrooms, changing rooms, bathrooms, sickbays, or examination venues—is strictly banned, constitutes severe gross misconduct, and will be escalated to law enforcement where necessary.

8. RULES FOR APPROPRIATE & UNACCEPTABLE NETWORK USE

8.1 Acceptable Use

Users are expected to make appropriate use of internet facilities and connectivity primarily for direct educational purposes, academic research, and constructive communication. General school rules for behavior and communication apply fully to digital environments.

8.2 Unacceptable Network & System Use

The following activities are strictly prohibited on all school computers, personal devices on campus, and network facilities:

1. **Offensive & Harassing Language:** Using impolite, anti-social, profane, abusive, racist, sexist, or hate speech in any electronic message, email, or post.
2. **Unauthorized Surfing & Chat Rooms:** Accessing chat rooms, gaming sites, or web facilities that have no relevance to assigned educational projects during academic time.
3. **Pornography & Explicit Material:** Accessing, downloading, storing, or distributing pornographic, sexually explicit, violent, crude, or socially unacceptable text, graphics, or videos.
4. **Spamming & Mail-Bombing:** Sending chain letters, spam, or mail-bombing server accounts.
5. **Account Impersonation & Fraud:** Using or attempting to use another user's login or credentials. Should a user find a computer left logged in by someone else, they must notify a staff member immediately and must not access files, change settings, or impersonate that user. Passwords must never be shared.
6. **Hacking & System Interference:** Attempting to hack into accounts, bypass school firewalls or content filters (e.g., via VPNs), break into network directories, or deploy viruses/malware.





7. **Software Piracy & Unauthorized Software:** Copying, installing, or downloading games, pirated software, media files, or unauthorized applications onto network drives or school computers. Piracy is a criminal offense.
8. **Hardware Tampering & Vandalism:** Tampering with, damaging, moving, or vandalizing school computer equipment, cables, or lab furniture, or altering default system configurations without written IT department approval.
9. **Movable Media Control:** Plugging flash drives, external hard drives, or memory cards into school computers without explicit teacher permission.

9. SOCIAL MEDIA, EXTRATERRITORIAL JURISDICTION & THE "SPILLOVER EFFECT"

1. **Public Domain Acknowledgment:** Items placed on social networking sites or transmitted electronically—even within private chat groups (e.g., WhatsApp, Discord, Telegram)—exist in the public domain and leave a permanent digital footprint.
2. **The "Spillover Effect" & Disciplinary Jurisdiction:**
 - While the school does not routinely monitor private off-campus devices or personal chat groups, participating in an off-campus chat provides **no immunity** from school disciplinary action.
 - If content created in a private digital space (e.g., screenshots, memes, voice notes, defamatory messages) leaks into the school environment, causes emotional or psychological distress, disrupts operations, or harms the school's reputation, Stanford Lake College reserves the explicit right to investigate and institute formal disciplinary proceedings.
3. **Legal Accountability in Chat Groups:** Under South African Common Law (*dignitas*) and the Cybercrimes Act, individuals who like, share, forward, or fail to repudiate defamatory or illegal content in digital chat groups can be held legally co-liable. Group administrators who fail to remove or condemn unlawful material face joint accountability.

10. WEB INTERACTIVE TOOLS, CLOUD SERVICES & PRIVACY

When using Web 2.0 tools, Google Suite, classroom blogs, or educational cloud platforms, users must observe all established safety guidelines:

- Cloud interaction is an extension of the classroom; classroom standards of respect apply.
- Users must never post personal identifiable information (last names, home addresses, phone numbers, personal photos) online without authorization.
- Users must never agree to meet someone they encountered online.
- Users must review all hyperlinked content before attaching links to academic blogs or posts to ensure appropriateness.





11. CONTRAVENTION, DISCIPLINARY CONSEQUENCES & ENFORCEMENT

Stanford Lake College takes any violation of this policy extremely seriously. **Any failure to comply with the guidelines, directives, or prohibitions outlined in this policy will result in formal disciplinary action.**

11.1 Monitoring & Device Inspection Rights

- **No Absolute Privacy on Network:** The IT Department reserves the right to audit, inspect, and monitor any email, network drive, or network traffic where non-compliance with school policy is suspected.
- **Device Search Rights:** As detailed in *Annexure K*, where reasonable suspicion of policy contravention, unauthorized content, cyberbullying, or academic dishonesty exists, **the school reserves the explicit right to inspect personal electronic devices in the presence of the owner**, and any retrieved evidence may be used in formal disciplinary hearings or criminal investigations.

11.2 Sanctions for Learners

Contravention by a pupil will be investigated under the Learner Code of Conduct. Consequences include:

- Official written warnings and demerits.
- Immediate device confiscation (minimum 1 week for general campus breaches; longer for repeated infractions).
- Revocation of network access privileges (the school is not required to provide alternative equipment for assessment tasks during penalty periods).
- Mandatory parent-school disciplinary conferences.
- Formal Disciplinary Hearings.
- Suspension or **Expulsion** for gross misconduct (e.g., severe cyberbullying, CSAM distribution, hacking, gross disrepute).

11.3 Sanctions for Staff

Contravention by an employee will be investigated under the Staff Disciplinary Code. Consequences include:

- Formal written warnings and final written warnings.
- Formal Disciplinary Hearings.
- **Summary Dismissal** for gross misconduct (e.g., boundary erosion, improper contact with learners, breach of confidentiality, gross insubordination, or reputational damage).
- Reporting to **SACE** (South African Council for Educators) and referral to the **NRSO** (National Register for Sex Offenders) where applicable.





11.4 Sanctions for Parents & External Parties

- Non-compliance, defamation, or harassment of staff/learners via digital platforms may result in formal legal warnings, restriction from campus, and **termination of the learner's enrollment contract**.
- Misuse or damage to school equipment by users or their children will result in financial liability for all repairs or replacements.

11.5 Statutory & Criminal Escalation

Where conduct involves statutory criminal offenses—such as cyberbullying under the Cybercrimes Act, distribution of CSAM, non-consensual intimate media sharing, extortion, or severe POPIA violations—Stanford Lake College is legally obligated to and **will immediately escalate the matter to the South African Police Service (SAPS), the Information Regulator, or Child Protection Authorities.**

