The Lawrence School, Sanawar

Digital Safety and Responsible Technology Use Policy.

Digital Safety and Responsible Technology Use Policy.

1. Objective:

- **Cyber safety & responsible digital use**
- **Prevention and response to cyberbullying**
- **Protection of children's physical, emotional, and online safety**

"This policy emphasizes prevention, early intervention, education, and restorative practices alongside disciplinary measures."

1.1 Student Code of Conduct:

All students are expected to act as responsible digital citizens. This includes treating others with the same respect online as they would in person. Specifically, students must refrain from using digital platforms to engage in cyberbullying, harassment, or the sharing of non-consensual imagery. Users are prohibited from attempting to bypass security filters, accessing inappropriate or age-restricted content, or impersonating others **whether on school-owned or personal devices while on campus.** Ethical use also requires respecting intellectual property and maintaining the privacy of peers and staff by not sharing personal information or photographs without explicit permission.

2. Scope

This policy applies to:

- All students (Boarders and Day Scholars).
- Teaching, Administrative, and the Support Staff.
- Parents/Guardians.
- Visitors using school digital systems or networks.

It covers:

- School-owned and personal devices.
- Internet access on campus.
- Online platforms, LMS, emails, and messaging tools.
- Social media and online behaviour impacting the school community.
- This policy applies during and outside school hours if the behaviour impacts the school community, its reputation, or student well-being.

3. Cyber Security & Online Safety Policy

3.1 Acceptable Use of Technology

All users must:

- Use technology for educational, administrative, or approved purposes only.
- Respect privacy, dignity, and rights of others.
- Follow the School Rules and the National Cyber Laws.

❖ **Cyberbullying** is the use of digital technologies, such as phones, computers, social media, or online gaming platforms, to harass, threaten, embarrass, or target someone. It can involve spreading rumours, sharing hurtful content, or impersonating others, and may cause serious emotional, psychological, and sometimes physical harm.

Users must NOT:

- Be involved in cyberbullying.
- Access or distribute inappropriate, violent, or explicit content.
- Attempt to bypass internet filters, firewalls, or security controls.
- Share passwords or impersonate others.
- Download or install unauthorized software.
- Engage in hacking or data misuse.
- Use AI tools for academic dishonesty, impersonation, or creation of harmful content.

3.2 Internet & Network Security

The School will:

- Use firewalls, content filters, and monitoring tools.
- Restrict access to unsafe websites.
- Monitor network usage for safety purposes.

❖ **No expectation of complete privacy on the school systems:**

Users should be aware that the school systems are monitored for safety and security purposes, in accordance with applicable laws.

3.3 Device Usage (Boarding)

- Device usage timings may be restricted.
- Devices may be collected at night as per the school rules.
- Random device checks may be conducted.
- Need base access to devices will be permitted under staff supervision.
- Any device confiscation will be documented and processed as per the school disciplinary procedure.

4. Online Bullying (Cyberbullying) Policy

4.1 Cyberbullying includes:

- Sending threatening or abusive messages.
- Spreading rumours, false information, or morphed images.
- Online shaming, trolling, or exclusion.
- Impersonation or misuse of another's identity.
- Repeated online harassment.
- Sharing screenshots or private conversations with intent to harm.

4.2 Zero Tolerance Approach

While cyberbullying is treated as serious misconduct, responses will be proportionate, age-appropriate, and focused on correction, accountability, and learning.

Actions may include:

- Counselling and warning.
- Suspension of digital access.
- Parents/Guardians notification.
- Suspension or Expulsion (for severe or repeated offences)

4.3 Reporting Cyberbullying

Students can report:

- To the DOF / Sr. Master, Sr. Mistress (GD/PD)
- To the Housemaster/ Housemistress/ Tutor and Matron.
- To the School Counsellor
- Via confidential reporting mechanism / email

5. Child Protection Policy: The school follows a 'CHILD FIRST' principle in all decisions.

5.1 Commitment to Child Safety

The school is committed to:

- Providing a safe, secure, and nurturing environment.
- Protecting children from abuse, neglect, exploitation, and harassment.
- Acting in the best interest of the child at all times.

5.2 Forms of Abuse Covered

- Physical abuse.
- Emotional or Psychological abuse.
- Sexual abuse or exploitation.
- Negligence.
- Online grooming or exploitation.

5.3 Child Protection Guidelines for the Staff

Staff must:

- Maintain professional boundaries with the students.
- Avoid all means of private or inappropriate online communication.
- Not share personal contact details without authorization.
- Immediately report any concern or suspicion.

5.4 Online Child Protection Measures

- Monitoring of all online platforms used by the students.
- Blocking of all unsafe content and platforms.
- Awareness programs on online grooming and predators.
- Restrictions on the social media usage (as per the School Rules).

6. Data Protection & Privacy

The school will:

- Protect personal data of the students and staff.
- Restrict access to sensitive information.
- Use secure systems for data storage and communication.
- Regular age-appropriate digital citizenship education will be integrated into the school curriculum.

Users must:

- Not share personal information online.
- Not upload photos/videos of others without consent.
- Respect confidentiality of the school.

7. Reporting & Incident Management

7.1 Reporting Channels

Incidents related to:

- Cyberbullying
- Online abuse
- Child safety concerns

Must be reported to:

- To the DOF / Sr. Master, Sr. Mistress (GD/PD)
- Housemaster/ Housemistress/Tutor and Matron
- School Counsellor
- Headmaster / DHM

Time Line:

- **Preliminary assessment within 24 hours.**
- **Investigation initiated within 48 hours.**

7.2 Response Procedure

The school will:

- Ensure immediate safety of the child.
- Conduct a confidential investigation as per the Child Protection and Disciplinary Policy of the School.
- Inform Parents/Guardians.
- Take disciplinary action as per the Schools Disciplinary Policy.
- Report to legal authorities if required.
- Provide counselling and support.

8. Training & Awareness

The school will conduct:

- Regular cyber safety workshops for students.
- Annual child protection training for the Staff.
- Awareness sessions for the parents.

9. Legal & Regulatory Compliance

This policy aligns with:

- Information Technology Act, 2000.
- Cyber Crime Prevention Guidelines.
- Child Protection Laws (including POCSO where applicable).

- CBSE safety guidelines.

10. Policy Violations & Consequences

Violations may result in:

- Disciplinary action as per the Disciplinary Policy of the School.
- Suspension of device or internet access.
- Legal action (if applicable).

11. Parent Partnership

Parents/Guardians are expected to:

- Monitor children's online behaviour when at home.
- Support school guidelines on device usage.
- Report concerns promptly.

12. Acknowledgement

All Students, Staff, and Parents/Guardians must acknowledge that they have read, understood, and agreed to comply with this policy.

The Policy may be reviewed after two years.

Made by:

Mr. H. Jamwal

HoF-IT

Vetted By:

Ravi Kumar

Deputy Headmaster

Approved by:

Himmat Singh Dhillon

Headmaster.

Date: 1st January, 2026

Date of Review: 1st January, 2028

13. Consent

I, ______________________ (Father/Mother) of ______________________, have read the policy in detail. I completely understand it and agree to adhere to all the terms and conditions mentioned therein.

Signature of Parents with date.