LOGISPARK TECHNOLOGIES PVT. LTD.

Employee Code of Conduct and Safeguarding Policy

Field	Detail	Field	Detail
Document owner	Managing Director	Version	3.0
Date of issue	11 January 2026	Effective from	11 January 2026
Approved by	Sayal Baidya	Next review	11 January 2028
Applies to	All employees, interns, contractors, consultants, associates and subcontractors of Logispark Technologies Pvt. Ltd., on every assignment and for every client.	Company Reg. No.	194168/075/076

1. Purpose and Scope

Logispark Technologies Pvt. Ltd. builds software for clients that include government institutions, non-governmental organisations, international development agencies, United Nations bodies and private sector companies in Nepal and internationally. Much of that work brings our people into contact with communities, beneficiaries, service users, patients, learners, customers and members of the public, including in field settings away from our office and away from supervision.

This Code sets out the standards of behaviour required of everyone working for or on behalf of Logispark, and the mechanism through which concerns about that behaviour can be raised and acted upon. It exists to protect the people we come into contact with, to protect our own staff, and to give every client confidence that their standards travel with us into the field.

This is a standing company policy. It applies to every assignment we undertake, for every client, whether or not that client requires a code of conduct, and whether or not an assignment involves community contact. It is not written for any single project and does not expire with one.

Who this Code applies to

- All employees of Logispark Technologies Pvt. Ltd. — permanent, probationary, part-time and fixed-term.
- Interns, trainees and volunteers.
- Contractors, freelance associates and consultants engaged by Logispark.
- Subcontractor organisations and their personnel working on a Logispark assignment.
- Directors and officers of the company.

Acceptance of this Code is a condition of employment or engagement. Every person to whom it applies signs the Acknowledgement and Undertaking at Appendix 1 before beginning work, and again on any material revision.

Relationship to client standards

Where a client organisation maintains its own code of conduct, safeguarding policy, child protection policy or reporting requirements, our personnel comply with that standard in addition to this Code for the duration of that assignment. Where the two differ, the stricter standard applies. Where a client requires our personnel to sign its own code, they do so, and this Code continues to apply alongside it.

2. Our Commitments

Logispark commits to the following and holds itself accountable for them.

- We treat every person we encounter through our work with dignity and respect, regardless of sex, gender identity, sexual orientation, caste, ethnicity, religion, disability, age, marital status, language, nationality, political opinion or economic status.
- We recognise that people may be placed at risk by contact with us, particularly children, people with disabilities and others in vulnerable circumstances, and we act to prevent that harm rather than waiting to respond to it.
- We operate a zero-tolerance position on sexual exploitation, sexual abuse and sexual harassment. There is no threshold of seniority, commercial value or project urgency that changes this.
- We create an environment in which concerns can be raised without fear, and we act on them.

- We report safeguarding concerns to the client organisation promptly and honestly, including when the concern reflects badly on us.
- We uphold the principles of human rights and gender equality, and we do not tolerate forced labour, bonded labour, child labour or any form of modern slavery in our operations or our supply chain.
- We treat the personal data of the people our clients serve as a safeguarding responsibility, not merely a technical one.

3. Standards of Professional Conduct

Everyone working for Logispark shall

- Act with honesty, integrity and professionalism in all dealings with clients, colleagues, partners and members of the public.
- Comply with the laws of Nepal and of any country in which they are working, and with the reasonable rules and instructions of any client institution whose premises they are on.
- Respect local customs, dress appropriately for the setting, and behave in a manner that does not cause offence to the community they are working in.
- Treat colleagues with courtesy, and neither engage in nor tolerate bullying, intimidation, discrimination or harassment of any kind.
- Perform their duties competently and to the standard the client has been promised.
- Report any concern arising under this Code through the mechanism in Section 10.

Everyone working for Logispark shall not

- Consume alcohol or any controlled substance while on duty, on client premises, or in a manner that impairs judgement during a field assignment.
- Carry or use weapons in the course of Logispark work.
- Use the company’s name, resources, systems or client relationships for personal gain.
- Make any commitment on behalf of a client that has not been authorised.
- Post to social media, or otherwise publish, images, video, data or information relating to a client, a project or a community member without documented authorisation and, where the person is identifiable, their informed consent.
- Engage in any behaviour prohibited by Sections 4 to 9 of this Code.

4. Safeguarding: Children and At-Risk Adults

A child is any person under the age of eighteen. An at-risk adult is any person aged eighteen or over who, by reason of disability, illness, age, displacement, poverty or other circumstance, may be unable to protect themselves from harm or exploitation.

Prohibited conduct

- Any form of physical, sexual, emotional or psychological abuse, neglect or exploitation of a child or at-risk adult.

- Any sexual activity with a person under eighteen, irrespective of the age of majority or age of consent in the location concerned, and irrespective of any claim of consent or of mistaken belief about age. Mistaken belief about a child's age is not a defence.
- Physical punishment or discipline of a child.
- Engaging a child in labour that is inappropriate, hazardous or interferes with their education.
- Photographing or filming a child without the documented consent of a parent or guardian and an explained, legitimate purpose.
- Sharing accommodation or sleeping in the same room as a child who is not one's own family member.
- Developing a relationship with a child or at-risk adult that could be interpreted as exploitative, or that involves secrecy from parents, guardians or colleagues.

Required practice

- Personnel avoid being alone and unobserved with a child or at-risk adult in the course of their work. Where contact is necessary, it takes place in an open setting or with a colleague or the person's guardian present.
- Personnel do not offer money, gifts, favours or employment to a child or at-risk adult, or to their family, outside a documented and approved programme arrangement.
- Personnel do not transport a child or at-risk adult alone in a vehicle other than in a genuine emergency, and report the circumstances afterwards.
- Personnel report any concern about the safety or welfare of a child or at-risk adult, whether or not it involves a Logispark colleague, through the mechanism in Section 10.

These requirements apply in all settings, including field visits, training sessions, community orientation events, user testing, data collection and onboarding activities, and whether or not the person concerned is a participant in the assignment.

5. Prevention of Sexual Exploitation, Abuse and Harassment

Definitions used in this Code

- Sexual exploitation: any actual or attempted abuse of a position of vulnerability, differential power or trust for sexual purposes, including profiting monetarily, socially or politically from the sexual exploitation of another.
- Sexual abuse: actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.
- Sexual harassment: any unwelcome conduct of a sexual nature, whether verbal, non-verbal, physical or digital, that has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment.

Prohibitions

- Sexual exploitation and sexual abuse of any person are prohibited absolutely and constitute grounds for summary dismissal and, where applicable, referral to the authorities.
- The exchange of money, employment, goods, services, preferential treatment or any other benefit for sex or sexual favours is prohibited. This includes any exchange of assistance owed to a person.
- Transactional sexual activity is prohibited while engaged on Logispark work, irrespective of local legality.

- Sexual relationships between Logispark personnel and beneficiaries, service users, community members or client staff encountered through an assignment are prohibited, because the inherent imbalance of power undermines the credibility of any claim of consent.
- Sexual harassment of colleagues, client personnel, partners or members of the public is prohibited, in person and through any digital channel including messaging applications, email and social media.

Obligation to report

Any person who develops a concern or suspicion of sexual exploitation, abuse or harassment by a colleague, a subcontractor, a partner or any other person encountered through our work is required to report it through the mechanism in Section 10. The obligation is to report a concern; it is not the reporter's responsibility to investigate, to gather proof, or to be certain before speaking.

6. Conduct During Field Assignments and Community Contact

Field assignments carry the highest safeguarding exposure in our work, because they place our personnel in communities, in homes and premises, and in settings where the people we meet did not choose to encounter us. The following applies to every field assignment, for every client.

Before deployment

- Every team member receives a safeguarding briefing covering this Code, the client's standards, the reporting mechanism and the specific context of the location. The briefing is recorded and the checklist at Appendix 2 is completed.
- The team is given the name and contact details of the Safeguarding Focal Point and the client's reporting route, in writing, before travelling.
- Reference and background checks appropriate to the role are completed before any person is assigned to field work involving community contact.

During the assignment

- Personnel visit homes, premises or households in pairs wherever practicable, and do not enter a private residence alone where a person is present alone, particularly a woman, a child or an at-risk adult.
- Personnel identify themselves clearly, explain the purpose of the visit, and make plain that participation is voluntary and that no service or entitlement depends on it.
- Personnel obtain informed consent before collecting any personal data, photograph or recording, explain how it will be used, and do not proceed if consent is refused.
- Personnel do not enter into private financial transactions with community members, and do not accept hospitality or gifts beyond ordinary courtesy such as tea.
- Personnel comply with the instructions of the client institution and of local authorities regarding access, timing and conduct.

After the assignment

- Any incident, concern or near-miss is reported through the mechanism in Section 10 within twenty-four hours of the team returning, or sooner where the matter is urgent.
- Personal data collected in the field is transferred to secure storage and removed from personal devices.

7. Anti-Fraud, Anti-Bribery and Anti-Corruption

- Logispark personnel shall not offer, promise, give, solicit or accept any bribe, kickback, facilitation payment or improper inducement, whether in cash or in kind, to or from any person, including public officials, client staff, procurement personnel or partner organisations.
- Personnel shall not attempt to influence a tender, evaluation or selection process by any improper means, and shall not misrepresent the company's capacity, experience, qualifications or costs in any proposal or report.
- Company and client funds, assets and equipment shall be used only for their authorised purpose, and all expenditure shall be supported by accurate records and genuine documentation.
- Gifts and hospitality shall not be offered or accepted where they could reasonably be seen to influence a business decision. Anything beyond modest, customary courtesy is declined, or declared to the Managing Director and recorded.
- Falsification of timesheets, invoices, expense claims, delivery records or project reports constitutes fraud and is grounds for dismissal.

8. Anti-Money Laundering

- Logispark receives and makes payments only through its registered corporate bank accounts. Cash payment or receipt for contracted work is not permitted.
- The company does not accept payment from, or make payment to, a third party that is not a contracting party to the engagement, without documented justification and approval.
- The company maintains accurate accounting records, issues compliant tax invoices, and complies with its obligations to the Inland Revenue Department and other competent authorities.
- Personnel shall report to the Managing Director any transaction, request or arrangement that appears designed to disguise the source, ownership or destination of funds.
- The company will provide beneficial ownership information to a client where required as part of due diligence.

9. Conflict of Interest, Confidentiality and Data Protection

Conflict of interest

A conflict of interest arises where a personal, financial, family or other outside interest could improperly influence, or be reasonably perceived to influence, the judgement a person exercises in their work.

- Personnel shall declare in writing to the Managing Director any actual, potential or perceived conflict of interest as soon as they become aware of it.
- Declarable interests include a family or close personal relationship with client or partner personnel involved in a selection, evaluation or approval decision; a financial interest in a competitor, supplier or subcontractor; and outside employment or consultancy bearing on a Logispark engagement.
- A person with a declared conflict is removed from the relevant decision, and the removal is recorded. The company maintains a conflict of interest register reviewed by the Managing Director.

Confidentiality and responsible use of information

Our work routinely involves access to client systems, personal data of community members and service users, and commercially sensitive information. Mishandling that access is itself a safeguarding failure, because the people whose data we hold are often those least able to absorb the consequences of its disclosure.

- Personnel access client data only to the extent required to perform their assigned task, and never out of curiosity or for personal purposes.
- Personal data is not copied to personal devices, personal cloud accounts or personal messaging applications, and is not retained after the task requiring it is complete.
- Client information, datasets, analyses, reports and outputs are treated as confidential and are not disclosed to any third party without the client's written approval.
- Production credentials are not shared between individuals, and access is revoked when a person leaves the assignment or the company.
- Any actual or suspected data breach is reported to the Managing Director and the affected client without delay, and in any event within twenty-four hours of discovery.
- Where a client requires a Data Processing Agreement or equivalent, it is signed before any development or data handling begins, and its terms bind every person on that assignment.
- Confidentiality obligations continue after the engagement or employment ends.

10. Reporting Concerns

A code that nobody can act on is decoration. This section sets out precisely how a concern is raised, by whom, and to whom.

10.1 Who can report

Anyone. Employees, interns, contractors and subcontractor personnel; client staff; partner organisations; and any member of the public, community member, beneficiary or service user who has had contact with Logispark personnel. A person does not need to be connected to Logispark to make a report, and does not need to identify themselves.

10.2 How to report

Channel	Contact	When to use
Safeguarding Focal Point	Anushka Maharjan anushka.maharjan@logisparktech.com +977 9841779580	The primary route for any safeguarding, PSEAH or conduct concern.
Deputy Safeguarding Focal Point	Prayush Shrestha prayush.shrestha@logisparktech.com +977 9843065157	Where the concern involves the Focal Point, or where the Focal Point is unavailable. The Deputy is of a different gender to the Focal Point so that a reporter may choose.
Confidential reporting address	safeguarding@logisparktech.com	Monitored only by the Focal Point and Deputy. Reports may be made anonymously.
Managing Director	Sayal Baidya, sayal.baidya@logisparktech.com +977 9818 0000 61	Where the concern involves both the Focal Point and the Deputy, or concerns fraud, bribery or money laundering.
Written report	Sealed envelope marked CONFIDENTIAL — SAFEGUARDING, addressed to the Safeguarding Focal Point at the registered office.	Where the reporter prefers not to use electronic means.
The client's own channel	Any person may report directly to the client organisation instead of, or in addition to, reporting to Logispark. For WaterAid assignments, WaterAid's reporting route applies.	Always available. A person is never required to report to Logispark first.

During field assignments, the name and mobile number of the Safeguarding Focal Point are provided in writing to the client's focal point and are made available to community members participating in orientation, training or data collection, in Nepali or the relevant local language.

10.3 What to include

A report is useful even when incomplete. Where the reporter is able, it helps to state what happened, when and where, who was involved, whether anyone is at immediate risk, and whether the reporter wishes to be contacted. A reporter is not expected to investigate, to gather evidence, or to be certain that their concern is well founded.

10.4 Immediate risk

Where a person is at immediate risk of harm, the first step is to ensure their safety and to contact the emergency services or the Nepal Police. The report to the Safeguarding Focal Point follows as soon as the immediate situation allows.

11. How Reports Are Handled

Stage	What happens
Acknowledgement	The Focal Point acknowledges receipt to the reporter within two working days, where the reporter is identifiable and contactable.
Immediate safety	Where any person may be at risk, immediate protective steps are taken before anything else, including suspending the individual concerned from contact with the affected person or from the assignment.
Notification to the client	Any safeguarding or PSEAH concern arising on a client assignment is reported to that client within twenty-four hours of receipt, whether or not it has been substantiated, and whether or not it reflects badly on Logispark. We do not investigate first and disclose afterwards.
Initial assessment	Completed within five working days: what is alleged, who is affected, whether a criminal offence may have occurred, and whether referral to the authorities is required.
Investigation	Conducted proportionately and impartially by a person with no involvement in the matter. Where the company lacks the necessary independence or expertise, an external investigator is appointed, or the matter is referred to the client or the authorities.
Outcome	The reporter is informed of the outcome so far as confidentiality and the rights of others permit. The client is informed of the outcome and of the action taken.
Record	A confidential record is maintained of every report, the action taken and the outcome, accessible only to the Focal Point and the Managing Director, and available to a client on request in the case of a concern arising on that client's assignment.

12. Protection of People Who Report

- No person will suffer dismissal, disciplinary action, demotion, exclusion from assignments, or any other detriment for making a report in good faith, whether or not the concern is subsequently substantiated.
- Retaliation against a reporter, a witness or a person who supports a report is itself a serious breach of this Code and is treated as a disciplinary matter in its own right.
- The identity of a reporter is disclosed only to those who need it in order to respond, and never to the person about whom the report is made, unless the reporter consents or the law requires it.
- Anonymous reports are accepted and acted upon, subject to the practical limits anonymity places on investigation.
- A report made maliciously or in bad faith, knowing it to be false, is a disciplinary matter. An honest concern that turns out to be mistaken is not.

13. Breaches and Consequences

A breach of this Code is a disciplinary matter. Depending on severity, consequences range from a written warning to summary dismissal, termination of a contract or subcontract, and referral to the Nepal Police or other competent authority.

Sexual exploitation, sexual abuse of any person, and any sexual activity with a child are grounds for summary dismissal and for referral to the authorities. Concealment of a known safeguarding concern, and retaliation against a person who reports, are treated with equivalent seriousness.

Where a breach occurs on a client assignment, Logispark will inform that client of the breach and of the action taken, and will cooperate fully with any investigation the client or the authorities conduct.

14. Subcontractors, Consultants and Associates

- Any subcontractor, consultant or associate engaged on a Logispark assignment is contractually bound to this Code, or to standards demonstrably equivalent to it, as a condition of engagement.
- Their personnel sign the Acknowledgement and Undertaking at Appendix 1 before beginning work.
- They are required to report concerns to the Logispark Safeguarding Focal Point on the same terms as our own staff.
- Failure to comply is grounds for immediate termination of the subcontract.

15. Training, Communication and Review

- Every new joiner receives a briefing on this Code as part of induction, before being assigned to any client work.
- Every team member deployed to a field assignment receives a context-specific safeguarding briefing before travelling, recorded on the checklist at Appendix 2.
- A refresher briefing is delivered annually to all personnel.
- This Code is reviewed at least every two years, and after any significant incident, by the Managing Director and the Safeguarding Focal Point.
- The current version is available to all personnel, is provided to clients on request, and may be submitted as part of any proposal or due diligence process.

Appendix 1: Acknowledgement and Undertaking

To be signed by every employee, intern, contractor, consultant and subcontractor before beginning work, and retained on file.

I confirm that:

- I have received, read and understood Logispark Technologies Pvt. Ltd. Employee Code of Conduct and Safeguarding Policy.
- I have had the opportunity to ask questions about it and to have them answered.
- I understand the standards of behaviour required of me, including the prohibitions on sexual exploitation, sexual abuse and sexual harassment, and the requirements relating to children and at-risk adults.
- I understand that I am required to report any concern arising under this Code, and I know how to do so and to whom.
- I understand that I must comply with the code of conduct and safeguarding standards of any client organisation on whose assignment I am working, and that where standards differ the stricter applies.
- I understand that a breach of this Code may result in disciplinary action up to and including summary dismissal or termination of contract, and may be referred to the authorities.
- I agree to be bound by this Code for the duration of my employment or engagement, and to maintain confidentiality obligations after it ends.

Field	Detail	Field	Detail
Full name		Date	
Designation/role		Assignment	
Employer/firm		Citizenship no.	
Signature		Briefed by	

Appendix 2: Field Assignment Safeguarding Briefing Checklist

Completed by the team leader before departure for any field assignment, and retained with the project record.

	Item	Confirmed (initial)
1	All team members have signed the Acknowledgement and Undertaking (Appendix 1).	
2	Reference and background checks appropriate to the role are complete for all team members having community contact.	
3	Team briefed on this Code and on the client's safeguarding standards.	
4	Team briefed on the specific context of the location: community, language, customs, sensitivities, local risks.	
5	Safeguarding Focal Point and Deputy names and mobile numbers issued to every team member in writing.	
6	Client reporting route issued to every team member in writing.	
7	Provide focal point contact details to the client focal point, and prepare them in the local language for community participants.	
8	Agreed consent procedure for any photography, recording, or personal data collection, with consent forms prepared in the local language.	
9	Pairing arrangement agreed for household or premises visits; lone-visit protocol understood.	
10	Emergency contacts recorded: Nepal Police, nearest health facility, client focal point, Logispark office.	
11	Data handling arranged: secure transfer, no personal devices retaining personal data after the assignment.	
12	Post-assignment reporting deadline understood: any incident, concern or near-miss reported within twenty-four hours of return.	

Field	Detail	Field	Detail
Client/assignment		Location	
Assignment dates		Team size	
Team leader		Signature	

Approved for and on behalf of Logispark Technologies Pvt. Ltd.

Sayal Baidya -
Managing Director
11 January 2026

Logispark Technologies Pvt. Ltd. · Company Reg. No. 194168/075/076