FAITH ACADEMY

Senior Secondary, Unaided Christian Minority School, Prasad Nagar, Delhi

MANUAL OF CHILD PROTECTION POLICIES

INDEX / TABLE OF CONTENTS

Sl. No.	Policy	Page No.
1	Child Protection & Safeguarding Policy	4
2	Child Protection Emergency Response Protocol	25
3	Anti-Bullying Policy	31
4	Cyber Security Policy	39
5	Student Transport Safety Protocol	54
6	Student Discipline Policy	61
7	Anti-Drug and Anti-Tobacco Policy	66

These policies were approved by the School Managing Committee in their meetings on 20.07.2026

FAITH ACADEMY

CHILD PROTECTION & SAFEGUARDING POLICY

“Take heed that ye despise not one of these little ones… it were better for him that a millstone were hanged about his neck, and that he were drowned in the depth of the sea.”
— Matthew 18:6, 10

Consolidated Edition — combining and superseding all prior versions of the Faith Academy and reference policies, and aligned to current Indian child-safeguarding law and regulatory guidance.

Document	Child Protection & Safeguarding Policy
Applies to	All staff (teaching, non-teaching, contractual, maintenance), Managing Committee, students, parents, volunteers, and visitors
Approved by	School Managing Committee
Review cycle	Annually, and immediately following any new central/state guidance, NCPCR direction, CBSE circular, or change in law
Aligned to	POCSO Act 2012 (as amended 2019) & POCSO Rules 2020; Juvenile Justice (Care & Protection of Children) Act 2015; RTE Act 2009; Child Labour (Prohibition & Regulation) Amendment Act 2016; POSH Act 2013; CBSE Affiliation Bye-Laws Chapter 4 (as amended July 2025); NCPCR Manual on Safety and Security of Children in Schools; UNCRC

PART 1 — POLICY STATEMENT, PURPOSE & COMMITMENT

1.1 Policy Statement

Faith Academy believes that every child has an inherent right to protection from harm, abuse, and exploitation. Children are gifts entrusted to us, and all adults who work with them carry a solemn responsibility to care for them with integrity, in a manner that honours their dignity, and that never violates their physical or emotional vulnerability.

Faith Academy employees, contractors, volunteers and partners are all engaged in a position of trust. When that trust is exploited, immense damage is caused to the child and to the wider community. Faith Academy therefore adopts a policy of Zero Tolerance towards the abuse or exploitation of children in any form.

This Policy sets out Faith Academy's commitment and responsibilities toward safeguarding children and protecting them from all forms of harm and abuse. Any form of harm or abuse of a child is unacceptable and non-negotiable. Any violation of this Policy — whether intentional or unintentional — will invite disciplinary action and, where applicable, referral to law enforcement, in accordance with this Policy and the law of the land.

Faith Academy equally recognises that its staff members need to be protected from false accusations and misunderstandings, and this Policy's procedures are designed to be fair and evidence-based for every party involved.

1.2 Purpose of the Policy

1.2.1 To promote and reinforce the school's commitment to safeguarding children.

1.2.2 To ensure that the safety, care, protection and welfare of the child are treated as paramount in everything the school does.

1.2.3 To provide a clear protection mechanism for all children engaged in Faith Academy's programmes and campus life.

1.2.4 To establish a standard code of conduct and standard procedures for all staff, contractual staff, maintenance staff and visitors, so that no harm or abuse is caused to any child.

1.2.5 To ensure that all staff, contractual workers, maintenance staff and visitors are informed, empowered and equipped to protect children and to respond appropriately to concerns.

1.3 Faith Academy's Commitment

1.3.1 **Awareness:** we will ensure that all staff, students, parents and partners are aware of the problem of child abuse and exploitation, the risks to children, the standards of behaviour they can expect from our representatives, and how to raise a concern.

1.3.2 **Prevention:** we will minimise risks to children through robust recruitment, training and supervision, and will create an environment where children's rights are respected and bullying, abuse or exploitation is prevented.

1.3.3 **Reporting:** we will ensure that staff and others are clear on the steps to take where concerns arise regarding the abuse or exploitation of a child.

1.3.4 **Responding:** we will ensure that appropriate, timely action is taken to support, safeguard and protect a child wherever concerns arise.

PART 2 — DEFINITIONS AND INDICATORS OF ABUSE

Child abuse is a general term describing inappropriate, immoral or unethical behaviour by an adult toward a person under 18 years of age, or by one child toward another child where a difference in power exists (for example, based on age, or physical, intellectual or emotional capacity, as in bullying). Abuse may occur with or without the consent of the victim, and in a one-to-one encounter or in a group setting. It is recognised under four categories below. Behavioural indicators alone do not prove abuse or neglect — they are signals that, taken together with other information, may warrant a closer look and should always be reported rather than investigated informally.

2.1 Physical Abuse

Inflicting physical injury on a child other than by accidental means — including bruising, burns, disfigurement, or impairment of physical or emotional health — or creating a substantial risk of such harm, including through excessive or degrading discipline or corporal punishment.

Indicators may include:

- Unexplained bruises, welts, burns, lacerations or fractures; bruising of differing ages/colours
- Injuries reflecting the shape of an object, or with a distinct immersion/rope-burn pattern
- Injuries inconsistent with the explanation offered, or that regularly appear after a break or holiday

2.2 Emotional Abuse

Treating a child in a way that deliberately undermines their confidence, self-esteem or self-worth — including name-calling, humiliation, threats, sarcasm, discrimination, withdrawal of love as punishment, or persistent ignoring of the child.

Indicators may include:

- Withdrawal, low mood, loss of appetite or motivation, mood swings, or avoidance of people and places

2.3 Sexual Abuse

The employment of physical and/or emotional sexual stimuli or acts in the presence of, or upon, an individual, with or without consent, or where the act is committed by a person in a position of trust regardless of consent. Sexual abuse falls into two categories:

2.3.1 **Touching offences —** including repeated touching, fondling, oral, genital or anal stimulation, and violent or non-violent sexual assault.

2.3.2 **Non-touching offences —** including indecent exposure, verbal sexual stimulation, voyeurism, causing a child to witness sexual acts, and exposure to pornographic material.

Indicators may include:

- Sexual knowledge or behaviour inappropriate to age; physical trauma to oral, genital or anal areas
- Difficulty walking or sitting; refusal to change for PE; fear of specific people or places

2. 4 Neglect

The failure, refusal or inability of a parent, guardian or other person exercising control over a child — for reasons other than poverty or war — to provide adequate food, clothing, shelter, supervision, or basic medical or emotional care, so as to endanger the child's wellbeing.

Indicators may include:

- Poor hygiene, ill-fitting clothing, persistent hunger, or being tired and physically small for age
- Parents/carers uninterested in or unreachable regarding the child's welfare

2.5 Grooming Behaviours

Staff and students alike should understand 'grooming'. Unlike most physical abuse, which is often impulsive, sexual abuse tends to be planned and secretive. A perpetrator typically grooms both the child and the surrounding organisation over time — becoming trusted and 'beyond reproach', while gradually building a 'special' relationship with a child that creates confusion, guilt or fear which discourages disclosure.

Warning signs may include:

- A staff member spending disproportionate or unsupervised time with one particular child
- A staff member giving a child special gifts, privileges, or unusual amounts of personal attention
- Excessive one-to-one online or off-hours contact with a child

2.6 Common Myths and Facts

Myth	Fact
Abuse is committed mostly by strangers	Around 90% of abuse is committed by someone known to the child — a parent, relative, carer, or staff member
Teaching children about abuse is harmful to them	Age-appropriate safety education makes children more confident and better able to respond to risk
Abuse only happens in poor or specific communities	Abuse occurs across every racial, ethnic, religious and socio-economic group
International/private schools are not required to report to local authorities	All schools are bound by host-country law and are liable, including criminally, for failure to report

PART 3 — GUIDING PRINCIPLES

Every safeguarding case is unique, and no set of guidelines can anticipate every circumstance. The following principles guide good judgement throughout:

3.1 Confidentiality: information is shared strictly on a need-to-know basis, both during an investigation and afterward. The child should be told clearly who will be informed of what they share.

3.2 Protection: every action prioritises the child's safety. Precautionary measures such as staff suspension are protective, not punitive or an assumption of guilt, and must be understood as such by all parties.

3.3 Prevention Awareness: the school continually reflects on its practices to identify and close safeguarding gaps, across gatekeeping, awareness, monitoring, reporting and responding.

3.4 Child-Centred Planning: the child's wishes and welfare are paramount and take precedence over any other competing interest or stakeholder priority.

3.5 Accountability & Responsibility: safeguarding is a whole-school responsibility. Roles differ by stage of the process, but everyone is accountable for reporting, whistle-blowing and safe practice.

PART 4 — STUDENT WELLBEING & ANTI-BULLYING FRAMEWORK

Safeguarding is strongest where it is built on a foundation of everyday student wellbeing, not only crisis response. Faith Academy's health and wellness programme aims to equip, motivate and support students to contribute positively to their own development and to the school community — building emotional, psychological, social and collective wellbeing, and maintaining a strict anti-bullying culture as an integral part of that wellbeing work.

4.1 Tiered Model of Support

Level of Intervention	Who is Involved
Whole-school culture, integrated into curriculum	Entire school community
General health/wellbeing curriculum	All students and teachers
Students needing additional support	Counsellor / Teacher / Wellness Ambassadors
Professional support	Counsellor / School Doctor / External specialists

This model informs assemblies, classroom discussions, peer 'Wellness Ambassador' programmes and staff CPD, and feeds directly into the Reporting and Responding protocols in Parts 8 and 9, so that wellbeing concerns and safeguarding concerns are never treated as separate silos.

PART 5 — PREVENTATIVE MEASURES

5.1 Dissemination and Awareness

5.1.1 Child protection training is mandatory for all staff — teaching, administrative, security, maintenance, and catering staff — and is included in new-staff orientation.

5.1.2 The Code of Conduct is displayed and every staff member signs a 'Declaration of Acceptance' before starting work.

5.1.3 An anonymous complaint mechanism (drop-box/addressed envelope) operates in every academic block.

5.1.4 CHILDLINE 1098 and the POCSO e-Box contact details are displayed prominently for students, staff and parents.

5.2 Recruitment and Selection

Recruitment reflects Faith Academy's commitment to safeguarding by screening out anyone unsuitable to work with children:

5.2.1 Verified references, with follow-up phone calls, and explanation required for any gap in employment history.

5.2.2 **Mandatory police / background verification:** in line with Rule 3 of the POCSO Rules, 2020, every staff member — teaching or non-teaching, regular or contractual — who is likely to come into regular contact with children undergoes police verification and character-antecedent checks, repeated periodically.

5.2.3 Support staff (drivers, conductors, peons, housekeeping, security) are engaged only through authorised, verifiable agencies, with records maintained on file.

5.2.4 All new staff, interns and volunteers sign the Child Protection Declaration of Acceptance and complete safeguarding training prior to any unsupervised contact with children.

5.3 Embedding Safeguarding into Management Systems

5.3.1 Safeguarding expectations are reflected in job descriptions, performance management and disciplinary procedures.

5.3.2 Off-campus activities (camps, field trips, sports fixtures) are risk-assessed and supervised to the same safeguarding standard as on-campus activities.

5.3.3 Marketing or media use involving children requires informed consent and must never increase a child's vulnerability.

5.4 Risk Assessment and Risk Management

All activities involving direct staff, visitor or parent contact with children — particularly one-to-one settings — are assessed to identify safeguarding risks and put adequate controls in place.

5.5 Information & Communication Technology

5.5.1 Staff must not have social contact with students or their parents through any medium, online or offline, unless specifically approved by the school.

5.5.2 Staff must not send social media friend/follow requests, or WhatsApp or other direct messages, to students beyond official classroom or subject-related communication channels.

5.5.3 Staff must not access or use children's social media profiles, photographs or personal content without approval from the appropriate school authority.

5.5.4 Children must not be exposed to unsuitable material in print or online, including content with sexual connotations, and staff must never show pornographic material to a child.

5.5.5 Cyber-crime, cyber-bullying and online-safety awareness training is provided to staff and students, including participation in national cyber-awareness initiatives.

5.6 CCTV and Physical Surveillance

In line with the CBSE amendment to Chapter 4 of the Affiliation Bye-Laws (July 2025), Faith Academy maintains high-resolution, audiovisual CCTV coverage of entry/exit points, corridors, staircases, lobbies, classrooms, laboratories, the library, canteen, storerooms and playgrounds, and all other common areas excluding washrooms and other areas requiring privacy.

5.6.1 Footage is monitored in real time where practicable and a minimum of 15 days of backup is retained and made available to appropriate authorities on request.

5.6.2 Staff are trained on privacy protocols and on using footage sensitively and only for safeguarding, safety or disciplinary purposes.

5.6.3 Parents and guardians are informed of surveillance arrangements as part of transparent communication about campus safety.

5.7 Learning and Development

Staff, parents and students are supported to build age- and role-appropriate safeguarding knowledge and skills, with child protection built into induction and ongoing mandatory training.

5.8 Audit and Review

This Policy, and each department's related procedures, is formally reviewed at least annually by the Managing Committee together with the Child Protection Committee, and immediately whenever new law, NCPCR guidance or CBSE circulars are issued, or whenever a case reveals a gap in current practice.

PART 6 — CREATING A PROTECTIVE ENVIRONMENT

A protective environment is the responsibility of every staff member, parent and partner — not of one person or a select group — and rests on five foundations: Gate-Keeping, Awareness & Sensitisation, Monitoring, Reporting, and Responding (each described in Parts 5, 8 and 9).

6.1 School Culture and Core Values

A safe school culture is built on a common mission, respectfulness, trustworthiness, openness, personal and organisational accountability, morality, inclusiveness, fairness, and objectivity. These values are refreshed regularly through assemblies, meetings and staff gatherings.

6.2 Designated Independent Contact Person

In addition to the Child Protection Officer (Part 8), Faith Academy nominates a respected adult who is known to the school community but who is not a member of staff, to serve as an independent contact person for students and parents. This person addresses the school assembly at least once each term, publishes their availability and contact number, and offers a channel for raising concerns outside the staff hierarchy.

6.3 General Guidelines on Verbal Interactions

6.3.1 Public reprimands of students or colleagues are kept to the minimum necessary to stop unsafe behaviour and must respect the dignity of the person concerned; detailed correction is given in private.

6.3.2 Sarcasm directed at students is avoided, as it is easily misunderstood and can undermine dignity.

6.3.3 Personal comments on ethnicity, social background, race or gender are never acceptable.

6.3.4 Escalating verbal confrontations are stopped and taken up later, or handed to a senior colleague.

6.3.5 Discussion of sex and sexual behaviour takes place only within the appropriate curricular context (health education, biology, or counsellor as relevant), never as jokes or casual remarks in front of students.

6.4 General Risk-Reduction Guidelines

6.4.1 A staff member or employee is alone with a child only in a location open to public view.

6.4.2 All students receive age-appropriate personal-safety instruction.

6.4.3 Staff maintain first-aid competence and know the emergency medical contact chain.

6.4.4 Students are actively encouraged to feel comfortable approaching any trusted adult with a safety concern.

6.4.5 Staff who feel they are under stress, or in a compromising situation, are encouraged to seek help without fear of judgement.

6.4.6 Any staff member concerned about a colleague's conduct raises it with the colleague directly or, in confidence, with the Child Protection Committee.

6.4.7 Selection and training of student council members and peer leaders (e.g. Wellness Ambassadors, Boy/Girl representatives) follows the same careful screening principles as staff selection.

PART 7 — CODE OF CONDUCT

7.1 All Staff, Contractual Staff and Visitors MUST:

7.1.1 Respect the privacy and dignity of every child, and be sensitive to age, gender, ethnicity, background, disability, sexuality and religion.

7.1.2 Proactively identify and manage safeguarding risks in every space accessed by children.

7.1.3 Create an environment where children are encouraged to discuss concerns about abuse or their rights, and always listen to and respect children's views.

7.1.4 Seek informed consent from children and parents/guardians before taking photographs, video, or formal interviews, and respect a child's right to say 'no' to being photographed or recorded.

7.1.5 Ensure any images or recordings of children are respectful of their dignity, with private body parts adequately covered.

7.1.6 Handle all child data and personal information with confidentiality, sharing publicly only with written authorisation from the school.

7.1.7 Ensure a staff member or other adult is alone with a child only in a location open to public view.

7.1.8 Report promptly any situation that might place a child at risk of harm.

7.2 All Staff, Contractual Staff and Visitors MUST NOT:

7.2.1 Abuse a child, or place a child at risk of harm, in any way.

7.2.2 Physically abuse, hit, or apply any form of corporal punishment to a child.

7.2.3 Intimidate, bully, humiliate, shame, threaten, coerce or belittle a child, or show differential/discriminatory treatment toward any child.

7.2.4 Hug, kiss or caress children, or engage in behaviour that is sexually provocative, offensive, or otherwise inappropriate.

7.2.5 Take a child to any private space or share a room with a child alone, except by counsellor in the counselling room and nurser or doctor in the medical room.

7.2.6 Have social contact with children or their parents through any medium, online or offline, unless approved by the school; send social media requests or WhatsApp/direct messages to students beyond classroom content; or access children's social media profiles or photographs without authorised approval.

7.2.7 Share personal contact details or a mobile number with a child without prior school permission.

7.2.8 Disclose a child's identity or personal information, or display/distribute images of a child without informed consent and school authorisation.

7.2.9 Take images or videos of children in secret or in a manner that could appear secretive.

7.2.10 Watch or show pornographic material in the presence of a child.

7.2.11 Engage in any substance use (alcohol, tobacco, drugs) in the presence of children.

7.2.12 Pass gifts to children other than through school-approved programmes, or give any gift without SMC approval.

7.2.13 Ask a child to perform personal errands or tasks that should be carried out by an adult.

7.2.14 Employ a child (as defined by law) in any capacity, official or personal, or patronise any service known to employ children unlawfully.

7.3 Additional Code of Conduct for Maintenance, Housekeeping and Support Staff

Given their distinct patterns of contact with children (washrooms, meal service, transport), maintenance and support staff observe the general Code of Conduct above, together with the following:

7.3.1 No maintenance or support staff member is alone with a child, except for a young child (pre-primary/primary) who has soiled their clothing or needs assistance reaching a washroom — and in such cases, female staff attend to girls and male staff attend to boys wherever possible.

7.3.2 Support staff (drivers, conductors, peons, housekeeping) are engaged only through authorised, verifiable agencies with full documentation on file.

7.3.3 Any emergency requiring a child to be taken off-site (e.g. medical attention) must be pre-approved by the school and appropriately chaperoned.

7.3.4 Maintenance and support staff sign the same Declaration of Acceptance (Annexure B) as teaching staff, tailored to their role.

7.4 Visitors and Parents on Campus

7.4.1 All visitors sign in, display identification, and are escorted or supervised while on campus, with access to children restricted outside of designated interaction areas.

7.4.2 Parents/guardians engaging with students other than their own must do so only through school-authorised channels.

PART 8 — REPORTING PROCEDURES

8.1 Duty to Report

Any adult who receives information about, witnesses, or has reason to suspect abuse of a child must report it to the Child Protection Officer without delay, and in writing, and in all cases the Principal will be notified. Even where there is doubt about the credibility of an allegation, it must still be reported accurately, completely and immediately — it is never the reporting adult's role to judge or investigate.

8.2 Managing a Disclosure — Listen, Record, Pass On

If a child begins to disclose abuse, tell them gently that you are glad to listen but that, because their safety matters, you will need to pass on anything they share about physical or sexual harm to the Child Protection Officer. Let the child share at their own pace; never probe for detail or express disbelief, however unlikely the account may sound. Your role is strictly to listen, record what was said as accurately as possible (using the child's own words where you can), and pass this on — not to investigate or judge.

8.3 The Child Protection Officer (CPO)

The school counsellor is recommended to serve as Child Protection Officer or a person deemed fit as per the school managing committee. The CPO receives and assesses all reports, and determines whether: (a) a child is at immediate risk and must be made safe without delay; (b) the child is currently safe but an allegation requires investigation; or (c) the information is too vague to act on immediately but should be logged for ongoing monitoring.

8.4 Reporting Log

All reports — verbal or written — are logged using the format below and forwarded to the Principal within 24 hours of discovery:

Reporter's name	Alleged victim & parent name(s)	Alleged perpetrator	How information was obtained	Details (date, time, place, what happened, direct quotes where possible)	Date reported	Who was contacted, when

Access to reports is restricted strictly to those who need to know in order to protect the child and progress the investigation.

8.5 External Reporting Channels

- **CHILDLINE 1098 —** 24-hour national emergency helpline for children.

- **POCSO e-Box —** NCPCR's online complaint system for direct reporting of sexual offences against children (ncpcr.gov.in/pocso).
- **Local Police / Special Juvenile Police Unit and the Child Welfare Committee (CWC) —** for formal complaints and statutory action.

In the event of sexual abuse, Faith Academy is mandatorily obligated under POCSO to report to the police (Women & Children's Unit); failure to report is itself a criminal offence.

PART 9 — INVESTIGATION AND RESPONSE PROTOCOL

Step 1 — Make Safe

A Child-at-Risk Meeting is convened without delay, comprising the Child Protection Officer, an SMC member and the Administrator on Duty. The Principal is notified of all actions and parents are informed. The meeting ensures the child is in a safe place and, as a precautionary (not disciplinary) measure, may suspend the staff member concerned pending investigation.

Step 2 — Investigation

The Principal appoints an investigation team — which may include external professionals — with balanced gender representation and no connection to either party in the allegation. The team gathers factual evidence only (not opinions), completes its work within 14 days, and, where relevant, arranges a medical examination through the School Doctor. Sexual abuse is reported to the police as a mandatory legal obligation; for physical abuse, reporting follows a criminal-offence threshold (e.g. assault causing bodily harm). Parents are updated at every stage, and strict confidentiality is maintained throughout.

Step 3 — Child Protection Hearing

A hearing, chaired by the Principal, is convened with a panel that may include an SMC member, an HOD, a faculty member and the school's legal counsel — none of whom were involved in the investigation. The panel reviews documentary and medical evidence and witness accounts as necessary, and decides: (a) whether abuse occurred; (b) what action is needed to protect and support the child and prevent recurrence; and (c) whether disciplinary action, criminal referral, or dismissal is warranted.

Step 4 — Follow-Up: Support and Prevention

Within two days of the hearing, the panel reconvenes to arrange support for the child and family, for affected staff and the wider community, and specialist support (therapists, doctors, police) as needed; to consider consulate notification for foreign-national families; and to take any wider safeguarding or awareness-raising action needed to prevent recurrence.

9.1 Outcomes

9.1.1 Where the investigation finds the allegation proven, the perpetrator's employment is terminated and the matter is referred to law enforcement as required by law.

9.1.2 Where an investigation is ongoing, the individual concerned may remain suspended, on a protective (not punitive) basis, until a decision is reached.

9.2 Special Circumstances

9.2.1 **Allegation against a parent (including a spouse/co-parent):** Steps 1–3 apply; home-country consulate/authorities may be notified where relevant, and legal guidance is sought before any restriction is placed on a parent's access to the school.

9.2.2 **Allegation against a visitor:** the visitor is immediately barred from campus and from any access to the child pending investigation and police referral.

9.2.3 **Allegation against a student:** the students involved are kept apart pending investigation; both sets of parents are notified; the alleged perpetrator may be separated or suspended to prevent further contact.

9.3 Support During Investigations

A designated staff supporter (without access to case details) supports any staff member under suspension and may accompany them to hearings. A designated student supporter, chosen for their existing positive relationship with the child, supports the student — again without access to investigation details. Both roles are strictly for welfare, not part of the investigation or disciplinary process.

PART 10 — GOVERNANCE: MANDATORY COMMITTEES

In line with CBSE norms, Faith Academy constitutes and displays (on notice boards and the school website) the composition and contact details of the following committees:

10.1 POCSO Committee

As constituted and approved

10.2 Internal Complaints Committee (POSH Act, 2013)

A separate Internal Complaints Committee handles complaints of sexual harassment involving adult members of staff at the workplace, under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. This is distinct from the POCSO Committee, which exists specifically to protect children.

10.3 School Wellbeing & Anti-Bullying Redressal Committee

Chaired by the Principal, with co-chair, counsellors, wellness teachers, coordinators and student Wellness Ambassadors, this committee oversees the tiered wellbeing model in Part 4 and handles bullying-related concerns that do not amount to abuse under POCSO.

10.4 Safety & Security Committee

Oversees CCTV and physical-security compliance, safety audits of premises, staff background/police-verification records, visitor-management systems, and periodic safety drills, reporting findings to the Managing Committee.

PART 11 — LEGAL FRAMEWORK IN INDIA

Faith Academy's policy operates within, and does not substitute for, the following legal framework:

(a) **Protection of Children from Sexual Offences (POCSO) Act, 2012, as amended 2019:** defines a child as any person under 18; criminalises sexual assault, harassment, and pornography involving children; makes failure to report a criminal offence; shifts the burden of proof onto the accused for the most serious offences; and (post-2019) allows for more stringent sentencing, including the death penalty for the gravest offences.

(b) **POCSO Rules, 2020:** require every institution in regular contact with children to conduct periodic police verification and background checks on all staff, and to organise periodic child-safety training.

(c) **Juvenile Justice (Care and Protection of Children) Act, 2015:** comprehensive legislation covering all children aged 0–18.

(d) **Right to Education Act, 2009:** free and compulsory education for children aged 6–14; prohibits physical and humiliating punishment.

(e) **Child Labour (Prohibition and Regulation) Amendment Act, 2016:** prohibits employment of children under 14 in any occupation, and of adolescents (14–18) in hazardous occupations.

(f) **Prohibition of Child Marriage Act, 2006**

(g) **Immoral Traffic (Prevention) Act, 1956:** criminalises trafficking of children for economic or sexual exploitation.

(h) **Information Technology Act, 2000:** covers production, dissemination and possession of child sexual abuse material.

(i) **United Nations Convention on the Rights of the Child (UNCRC):** India is a signatory.

11.1 Support and Oversight Bodies

- **CHILDLINE 1098 —** national 24-hour emergency helpline for children.
- **Child Welfare Committee (CWC) —** district-level quasi-judicial body deciding on custody/protection of children in need.
- **District Child Protection Unit (DCPU) —** district single-window body for awareness and protection.
- **State/National Commission for Protection of Child Rights (SCPCR/NCPCR) —** monitoring body for POCSO and RTE compliance, and publisher of the Manual on Safety and Security of Children in Schools.
- **Special Juvenile Police Unit —** designated police officers for child protection matters.

Mr. C. Sundaraj **Director** **Faith Academy Schools & Projects**	**Dr. M. Kannan** **Principal & Manager** **Faith Academy**	E. Robert **Mrs. E. Robert** **Principal & Manager** **Faith Academy Second Shift**

ANNEXURE A — DECLARATION OF ACCEPTANCE (STAFF & CONTRACTUAL EMPLOYEES)

I confirm that I have received and read the Faith Academy Child Protection Policy and Code of Conduct, and that I understand its principles, purpose and intent. I will always treat every child with respect, regardless of age, gender, disability, race, religion, sexual orientation or identity, and will support their right to equal protection from harm. I will not employ any child as defined under the Child Labour (Prohibition and Regulation) Amendment Act, 2016. I will report any case of child abuse, exploitation or neglect that comes to my knowledge to the appropriate authority without delay, and will not myself harm or abuse any child physically, emotionally or sexually. I understand that I am mandatorily required to report any concern about possible abuse or risk to a child, that I must adhere at all times to the Code of Conduct, and that any breach may result in disciplinary action, including termination and referral to law enforcement.

Name of Staff: ______________________________ Designation: ______________________

Signature: ______________________________ Date: ______________________

ANNEXURE B — DECLARATION OF ACCEPTANCE (MAINTENANCE & SUPPORT STAFF)

I confirm that I have received and read the Faith Academy Child Protection Policy, including the additional Code of Conduct for maintenance, housekeeping and support staff. I understand that I must never be alone with a child except where a young child (pre-primary/primary) requires help due to soiled clothing or a washroom visit, and that wherever possible female staff attend to girls and male staff attend to boys in such situations. I will respect the privacy and dignity of every child, will not photograph or video a child without appropriate consent, will not disclose any child's personal information, and will report immediately any situation that may place a child at risk.

Name of Staff: ______________________________ Role: ______________________

Signature: ______________________________ Date: ______________________

ANNEXURE C — QUICK-REFERENCE EMERGENCY CONTACTS

Contact	Details
Child Protection Officer	________________________ | Phone: ________________
Independent Contact Person (non-staff)	________________________ | Phone: ________________
Principal	________________________ | Phone: ________________
CHILDLINE	1098 (24-hour, toll-free)
POCSO e-Box	ncpcr.gov.in/pocso
Local Police / Special Juvenile Police Unit	________________________
Child Welfare Committee (CWC)	________________________

FAITH ACADEMY

CHILD PROTECTION EMERGENCY RESPONSE PROTOCOL

1. Purpose and Scope

This protocol translates Parts 8 and 9 of the Faith Academy Child Protection & Safeguarding Policy into a clear, actionable emergency response sequence for any member of staff, contractor, or visitor who becomes aware of, suspects, or witnesses possible abuse, neglect, or a safeguarding risk to a child. It does not replace the Policy — it is the field-ready summary of it. Where any conflict arises, the full Policy governs.

This protocol applies at all times a child is on campus, in transport, on an off-campus school activity, or otherwise in the care of Faith Academy staff or partners.

2. Golden Rules Before You Begin

2.1 Do not delay. If a child is in immediate danger or hurt, act to make them safe first — before any paperwork.

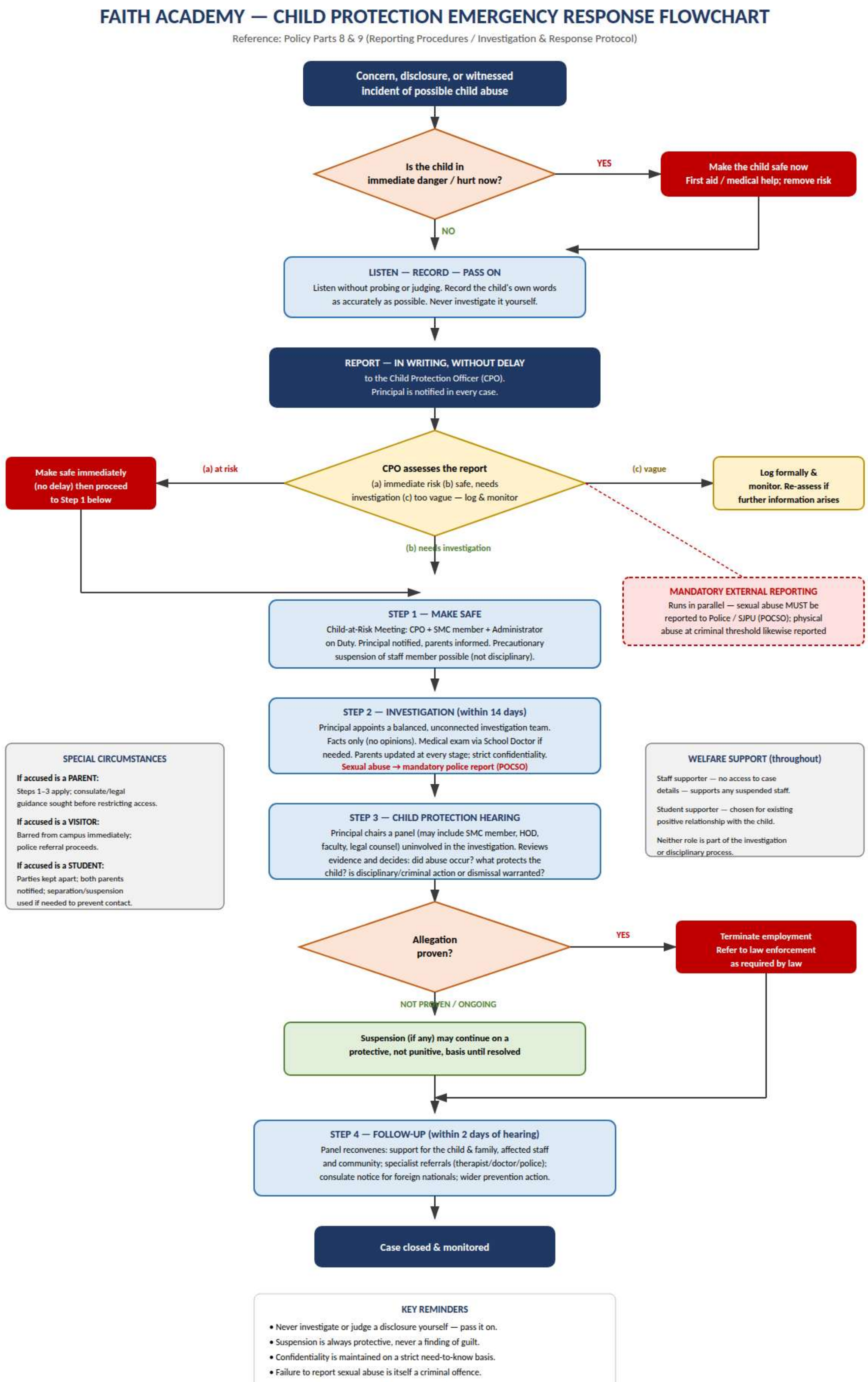
2.2 Do not investigate. It is never the reporting adult's role to judge, probe, or decide if an allegation is credible.

2.3 Do not promise secrecy. Tell the child gently that anything about physical or sexual harm must be passed on to protect them.

2.4 Always report in writing, without delay. Even where you have doubts about the account, report it accurately, completely, and immediately.

2.5 Suspension is protective, not punitive. It is never to be treated or communicated as a finding of guilt.

3. Step-by-Step Emergency Response Flowchart



4. Detailed Procedure

4.1 Immediate Safety Check

On becoming aware of a concern, first ask: is the child in immediate danger or in need of urgent medical attention? If yes, make the child safe without delay — remove them from the risk, provide first aid, or call emergency medical help as needed. Do not wait for a form or a meeting before acting to protect the child.

4.2 Managing a Disclosure — Listen, Record, Pass On

If a child begins to disclose abuse, gently explain that you are glad to listen, but that because their safety matters, anything they share about physical or sexual harm will need to be passed on to the Child Protection Officer (CPO). Let the child share at their own pace. Never probe for detail, never express disbelief, and never promise confidentiality you cannot keep. Your role is strictly to listen, to record what was said as accurately as possible using the child's own words wherever you can, and to pass this on — not to investigate or judge.

4.3 Report to the Child Protection Officer, in Writing, Without Delay

Any adult who receives information about, witnesses, or has reason to suspect abuse must report it to the CPO without delay and in writing. The Principal is notified in all cases. Even where there is doubt about the credibility of an allegation, it must still be reported accurately, completely and immediately.

4.4 CPO Assessment

The CPO receives and assesses every report and determines one of three pathways:

(a) The child is at immediate risk and must be made safe without delay.
(b) The child is currently safe, but the allegation requires investigation.
(c) The information is too vague to act on immediately, but is logged for ongoing monitoring and reassessed if further information arises.

4.5 Mandatory External / Statutory Reporting (runs in parallel)

Where the concern involves sexual abuse, Faith Academy is mandatorily obligated under POCSO to report to the police (Women & Children's Unit); failure to report is itself a criminal offence. Physical abuse is reported where it meets a criminal-offence threshold (e.g. assault causing bodily harm). This external reporting runs alongside, not instead of, the internal steps below. External channels include:

- CHILDLINE 1098 — 24-hour national emergency helpline for children.
- POCSO e-Box — NCPCR's online complaint system (ncpcr.gov.in/pocso).
- Local Police / Special Juvenile Police Unit and the Child Welfare Committee (CWC).

Step 1 — Make Safe

A Child-at-Risk Meeting is convened without delay, comprising the CPO, an SMC member, and the Administrator on Duty. The Principal is notified of all actions and parents are informed. The meeting ensures the child is in a safe place and, as a precautionary — not disciplinary — measure, may suspend the staff member concerned pending investigation.

Step 2 — Investigation (within 14 days)

The Principal appoints an investigation team — which may include external professionals — with balanced gender representation and no connection to either party. The team gathers factual evidence only, completes its work within 14 days, and arranges a medical examination through the School Doctor where relevant. Parents are updated at every stage, and strict confidentiality is maintained throughout.

Step 3 — Child Protection Hearing

A hearing, chaired by the Principal, is convened with a panel (which may include an SMC member, an HOD, a faculty member, and the school's legal counsel) — none of whom were involved in the investigation. The panel reviews the evidence and decides: (a) whether abuse occurred; (b) what action is needed to protect and support the child and prevent recurrence; and (c) whether disciplinary action, criminal referral, or dismissal is warranted.

Step 4 — Follow-Up: Support and Prevention (within 2 days of the hearing)

The panel reconvenes to arrange support for the child and family, for affected staff and the wider community, and specialist support (therapists, doctors, police) as needed; to consider consulate notification for foreign-national families; and to take any wider safeguarding or awareness-raising action needed to prevent recurrence.

4.6 Outcomes

4.6.1 Where the allegation is proven, the perpetrator's employment is terminated and the matter is referred to law enforcement as required by law.

4.6.2 Where an investigation is ongoing, the individual concerned may remain suspended, on a protective (not punitive) basis, until a decision is reached.

5. Roles and Responsibilities at a Glance

Role	Responsibility in an Emergency
Any Staff / Contractor / Visitor	Make the child safe if in immediate danger; listen, record, pass on; report to CPO in writing without delay.
Child Protection Officer (CPO)	Receives and assesses every report; decides immediate-risk / investigate / monitor pathway; convenes Child-at-Risk Meeting.
Principal	Notified in every case; appoints the investigation team; chairs the Child Protection Hearing.
SMC Member / Administrator on Duty	Participates in the Child-at-Risk Meeting (Step 1).
Investigation Team	Gathers factual evidence only, within 14 days; arranges medical examination if needed.
Hearing Panel	Decides whether abuse occurred and what action — protective, disciplinary, or criminal — is warranted.
Staff Supporter / Student Supporter	Provide welfare support only, with no access to case details; not part of the investigation.

6. Special Circumstances

6.1 **Allegation against a parent (including a spouse/co-parent):** Steps 1–3 apply; home-country consulate/authorities may be notified where relevant, and legal guidance is sought before any restriction is placed on a parent's access to the school.

6.2 **Allegation against a visitor:** the visitor is immediately barred from campus and from any access to the child, pending investigation and police referral.

6.3 **Allegation against a student:** the students involved are kept apart pending investigation; both sets of parents are notified; the alleged perpetrator may be separated or suspended to prevent further contact.

Support During Investigations

A designated staff supporter (without access to case details) supports any staff member under suspension and may accompany them to hearings. A designated student supporter, chosen for their existing positive relationship with the child, supports the student — again without access to investigation details. Both roles are strictly for welfare, not part of the investigation or disciplinary process.

7. Quick-Reference Emergency Contacts

Contact	Purpose
Child Protection Officer (CPO)	First point of contact for every internal safeguarding report.
Principal	Notified in all cases; appoints investigation team and chairs hearing.
CHILDLINE — 1098	24-hour national emergency helpline for children.
POCSO e-Box — ncpcr.gov.in/pocso	NCPCR's online complaint system for reporting sexual offences against children.
Local Police / Special Juvenile Police Unit	Formal complaints and statutory action; mandatory for sexual abuse.
Child Welfare Committee (CWC)	District-level body for custody/protection decisions.
School Doctor / Medical Emergency Contact	First aid, urgent medical care, and medical examinations during investigations.

Note: This protocol is a working summary for emergency use. Staff should refer to the full Faith Academy Child Protection & Safeguarding Policy (Consolidated Edition), Parts 8–9 and Annexure C, for complete detail, and should never rely on this summary alone to determine legal or disciplinary outcomes.

Mr. C. Sundaraj
Director
Faith Academy Schools & Projects

Dr. M. Kannan
Principal & Manager
Faith Academy

E. Robert
Mrs. E. Robert
Principal & Manager
Faith Academy Second Shift

FAITH ACADEMY

ANTI-BULLYING POLICY

1. Policy Statement

Faith Academy Senior Secondary School is committed to providing a safe, secure, inclusive, and caring learning environment where every student is treated with dignity and respect. The School maintains a zero-tolerance approach towards bullying in any form and is committed to preventing, identifying, addressing, and eliminating bullying through education, awareness, early intervention, and appropriate disciplinary measures.

Every student has the right to learn in an environment free from fear, intimidation, harassment, discrimination, and violence.

2. Purpose

The objectives of this Policy are to:

- Promote a culture of mutual respect, kindness, empathy, and inclusion.
- Prevent bullying and harassment in all forms.
- Protect the physical, emotional, social, and psychological well-being of students.
- Provide clear procedures for reporting and investigating bullying incidents.
- Ensure fair, prompt, and confidential handling of complaints.
- Encourage students, parents, teachers, and staff to work collaboratively in preventing bullying.
- Support victims, reform perpetrators, and educate bystanders.

3. Scope

3.1 Persons Covered

This Policy applies to:

- All students.
- Teachers.
- Non-teaching staff.
- School management.
- Volunteers.
- Visitors.

3.2 Settings Covered

The Policy shall apply:

- Within school premises.
- During school transportation.
- During educational tours, excursions, camps, competitions and school events.
- During online classes.

- On social media or digital platforms whenever such conduct adversely affects the school environment or the safety and well-being of any student.

4. Definition of Bullying

Bullying refers to intentional aggressive behaviour that involves an imbalance of power and is generally repeated over time. It causes physical injury, emotional distress, humiliation, intimidation, fear, or social exclusion.

Bullying may be committed by:

- One student against another;
- A group against an individual;
- One group against another group.

5. Forms of Bullying

Bullying includes, but is not limited to, the following categories:

5.1 Physical Bullying

- Hitting
- Kicking
- Pushing
- Slapping
- Tripping
- Damaging personal belongings
- Physical intimidation

5.2 Verbal Bullying

- Name-calling
- Mocking
- Teasing
- Insults
- Abusive language
- Threats
- Offensive remarks

5.3 Social or Relational Bullying

- Spreading rumours
- Gossiping
- Deliberate exclusion
- Public humiliation
- Manipulating friendships

- Encouraging others to isolate a student

5.4 Emotional Bullying

- Intimidation
- Harassment
- Ridicule
- Humiliation
- Continuous criticism
- Deliberate embarrassment

5.5 Cyber Bullying

Bullying carried out through electronic means including:

- Social media
- Messaging applications
- Emails
- Online games
- Fake accounts
- Sharing photographs or videos without consent
- Posting offensive comments
- Threatening messages
- Digital impersonation

6. Behaviour Not Tolerated

The School strictly prohibits:

- Physical assault
- Threats
- Harassment
- Intimidation
- Discrimination
- Hazing
- Extortion
- Rumour spreading
- Social exclusion
- Cyber harassment
- Retaliation against anyone reporting bullying
- Encouraging or supporting bullying

7. Rights of Students

Every student has the right to:

- Learn in a safe environment.
- Be treated with dignity and respect.
- Feel physically and emotionally secure.
- Report bullying without fear.
- Receive fair treatment.
- Receive appropriate support and counselling.

8. Responsibilities of Students

Every student shall:

- Treat everyone with kindness, dignity and respect.
- Refrain from engaging in any form of bullying.
- Respect differences relating to religion, race, gender, language, nationality, disability, academic performance, appearance or socio-economic background.
- Speak out against bullying.
- Report bullying immediately to a teacher, counsellor, House Coordinator or Principal.
- Support students affected by bullying.
- Act as responsible digital citizens.

9. Responsibilities of Parents

Parents shall:

- Encourage respectful behaviour.
- Discuss bullying awareness with their children.
- Cooperate with the School during investigations.
- Inform the School if they become aware of bullying.
- Support corrective interventions recommended by the School.

10. Responsibilities of Teachers and Staff

Teachers and staff shall:

- Maintain vigilance.
- Intervene promptly.
- Report incidents immediately.
- Maintain confidentiality.
- Promote a respectful classroom culture.

- Participate in anti-bullying awareness programmes.

11. Reporting Procedure

Any student, parent, teacher, staff member or witness may report bullying through:

- Class Teacher
- School Counsellor
- Head Mistress
- Administrative Officer
- Vice Principal
- Principal
- Written complaint
- Email
- Anonymous reporting mechanism (where available)

All reports shall be treated seriously.

12. Investigation Procedure

Upon receiving a complaint, the school shall:

- Record the complaint.
- Conduct a preliminary assessment.
- Interview the complainant.
- Interview the alleged offender.
- Interview witnesses.
- Review documentary or digital evidence.
- Maintain confidentiality.
- Record findings.
- Recommend appropriate action.

13. Support Measures

The School may provide:

- Counselling.
- Behavioural intervention.
- Parent meetings.
- Peer mediation (where appropriate).
- Safety plans.
- Classroom monitoring.

- Psychological support.

14. Disciplinary Measures

Depending upon the seriousness and recurrence, disciplinary action may include:

- Verbal warning.
- Written warning.
- Written apology.
- Counselling.
- Behaviour improvement plan.
- Community service.
- Parent conference.
- Suspension from specific activities.
- Suspension from school.
- Recommendation for expulsion in extreme cases, subject to applicable laws and school regulations.

Cyber bullying involving criminal offences may be reported to law enforcement authorities.

15. Protection Against Retaliation

No student shall suffer retaliation for:

- Reporting bullying;
- Assisting an investigation;
- Acting as a witness.

Any retaliatory act shall itself constitute serious misconduct.

16. Awareness and Prevention

The School shall promote:

- Anti-bullying campaigns.
- Classroom discussions.
- Orientation programmes.
- Digital safety education.
- Student leadership initiatives.
- Parent awareness workshops.
- Teacher training.

17. Confidentiality

All complaints and investigations shall be handled confidentially to the extent permitted by law and necessary for a fair investigation.

18. Student Anti-Bullying Pledge

Every student is encouraged to affirm the following pledge:

> *"I will treat every person with kindness, dignity and respect. I will not participate in verbal, physical, emotional, social or cyber bullying. I will support students who are affected by bullying, report incidents promptly, and help create a safe, respectful and caring school environment."*

19. Policy Review

This Policy shall be reviewed annually or earlier if required due to changes in law, educational guidelines, or institutional requirements.

20. Approval

This Anti-Bullying Policy has been approved and adopted by the School Managing Committee of Faith Academy at its meeting held on 20 July 2026 and shall come into force with immediate effect unless otherwise specified.

21. Publication and Acknowledgement

This Policy shall be:

- Published on the School's official website.
- Made available in the School Library and Administrative Office.
- Circulated to all employees through official communication channels.
- Explained during induction and periodic cyber safety awareness programmes.
- Acknowledged by every employee, who shall confirm that he or she has read, understood, and agrees to comply with the provisions of this Policy.

Failure to acknowledge receipt of this Policy shall not exempt any employee from compliance with its provisions.

Mr. C. Sundaraj **Director** **Faith Academy Schools & Projects**	**Dr. M. Kannan** **Principal & Manager** **Faith Academy**	E. Robert **Mrs. E. Robert** **Principal & Manager** **Faith Academy Second Shift**

FAITH ACADEMY

CYBER SECURITY POLICY

1. Purpose

Faith Academy is committed to maintaining a secure, resilient, and trustworthy digital environment for all stakeholders. The purpose of this Cyber Security Policy ("Policy") is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of the School's information assets, computer systems, communication networks, digital infrastructure, and electronic records against cyber threats, unauthorized access, misuse, loss, alteration, or destruction.

This Policy seeks to:

a. safeguard institutional, employee, student, parent, and other confidential information from cyber security risks;
b. establish uniform standards for the secure use of information and communication technology (ICT) resources;
c. prevent unauthorized access to, disclosure of, modification of, or destruction of digital information;
d. ensure compliance with applicable laws, Government of India advisories, and directions issued by the Ministry of Electronics and Information Technology (MeitY), the Indian Computer Emergency Response Team (CERT-In), the Directorate of Education, and other competent authorities;
e. promote cyber security awareness and responsible digital behaviour among all personnel;
f. minimize operational, financial, legal, and reputational risks arising from cyber incidents; and
g. establish clear responsibilities for preventing, reporting, and responding to cyber security incidents.

2. Scope

This Policy shall apply to:

a. all teaching staff;
b. all non-teaching staff;
c. the Principal, Manager, and members of the School Administration;
d. contractual employees;
e. outsourced personnel, including security personnel, housekeeping staff, maintenance staff, and other service providers having access to School systems or information;
f. consultants, interns, volunteers, and any other individual authorized to use the School's information systems.

The provisions of this Policy shall apply irrespective of whether official work is performed from School premises, remote locations, or through mobile devices.

This Policy shall govern the use of:

a. desktop computers;
b. laptops;
c. mobile phones;
d. tablets;
e. servers;
f. printers;

g. storage devices;
h. email services;
i. cloud platforms;
j. internet services;
k. Wi-Fi networks;
l. School software applications;
m. digital communication platforms; and
n. all other ICT resources owned, leased, or authorized by the School.

3. Definitions

For the purposes of this Policy, unless the context otherwise requires:

3.1 "Cyber Security"

means the practice of protecting digital systems, networks, applications, devices, and information from cyber-attacks, unauthorized access, misuse, damage, or disruption.

3.2 "Information Assets"

include all electronic records, databases, documents, software, hardware, cloud services, communication systems, passwords, and digital resources belonging to or used by the School.

3.3 "Confidential Information"

includes, but is not limited to:

a. student records;
b. employee records;
c. examination materials;
d. financial information;
e. payroll information;
f. bank details;
g. medical records;
h. passwords;
i. login credentials;
j. administrative records;
k. management communications; and
l. any information classified by the School as confidential.

3.4 "Official Device"

means any computer, laptop, tablet, mobile phone, storage device, or other electronic equipment owned, leased, or authorized by the School.

3.5 "User"

means any individual authorized to access or use the School's ICT resources.

3.6 "Cyber Incident"

means any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of information systems, including but not limited to phishing, malware infection, ransomware, hacking, unauthorized access, data leakage, identity theft, or theft of electronic devices.

4. General Responsibilities

Every user shall exercise due care and diligence while accessing, processing, storing, transmitting, or handling School information.

All users shall:

a. comply with the provisions of this Policy;
b. use School ICT resources solely for authorized purposes;
c. protect confidential information from unauthorized disclosure;
d. immediately report any suspected cyber security incident;
e. cooperate with investigations conducted by the School;
f. participate in cyber security awareness and training programmes organized by the School; and
g. comply with all lawful directions issued by the School regarding cyber security.

Failure to comply with this Policy may result in disciplinary action in accordance with the applicable service rules and other governing regulations.

5. Password Security

Passwords constitute the first line of defence against unauthorized access and shall therefore be created, maintained, and protected with the highest degree of care.

5.1 Every user shall:

a. create passwords consisting of a minimum of eight (8) characters incorporating uppercase letters, lowercase letters, numerals, and special characters;
b. use unique passwords for different systems and accounts;
c. change passwords at intervals not exceeding forty-five (45) days or immediately upon suspicion of compromise;
d. ensure that passwords are not predictable, easily guessed, or based upon personal information such as names, dates of birth, telephone numbers, or employee identification numbers;
e. maintain the confidentiality of passwords at all times; and
f. immediately change any password that is suspected of having been disclosed or compromised.

5.2 No user shall:

a. disclose passwords to any other person;
b. permit another individual to access official systems using his or her credentials;
c. write passwords on paper, sticky notes, diaries, or other unsecured media;
d. store passwords in unencrypted electronic files; or
e. reuse passwords previously used for official accounts where technically restricted.

Where technically feasible, the use of secure password management solutions approved by the Information Technology Department may be permitted.

6. Multi-Factor Authentication (MFA)

To strengthen the security of user accounts and reduce the risk of unauthorized access resulting from compromised passwords, Multi-Factor Authentication (MFA) shall be enabled wherever such functionality is available.

The Information Technology (IT) Department shall ensure, to the extent technically feasible, that MFA is implemented for all critical information systems.

All users shall enable and use MFA for, including but not limited to:

a. official email accounts;
b. cloud-based storage and collaboration services;
c. School portals and learning management systems;
d. financial and accounting applications;
e. administrative and human resource management systems; and
f. any other application designated by the School as requiring enhanced security.

Users shall not disable, bypass, or interfere with MFA without the prior written approval of the IT Department.

7. Software Updates and Patch Management

The timely installation of software updates and security patches is essential for protecting the School's information systems from known vulnerabilities.

Accordingly:

a. all operating systems installed on official devices shall be maintained with the latest security updates supported by the manufacturer;
b. security patches shall be installed promptly after release, subject to operational requirements;
c. antivirus and endpoint protection software shall remain active and updated at all times;
d. only software approved or licensed by the School shall be installed on official devices; and
e. obsolete or unsupported software shall be removed or upgraded as soon as practicable.

Employees shall not intentionally postpone, disable, or interfere with mandatory software updates issued by the IT Department.

Where updates require temporary interruption of work, employees shall cooperate with the IT Department to facilitate timely installation.

8. Antivirus and Endpoint Protection

The School shall implement appropriate antivirus and endpoint security solutions on all official devices to safeguard against malware, ransomware, spyware, viruses, and other malicious software.

8.1 The IT Department shall:

a. install and maintain licensed antivirus software on all official devices;
b. ensure that antivirus definitions and security signatures are updated regularly;

c. perform scheduled malware scans and vulnerability assessments;
d. monitor endpoint security alerts and respond to identified threats; and
e. isolate infected systems where necessary to prevent further compromise.

Employees shall:

a. permit scheduled antivirus scans to run without interruption;
b. immediately report any malware warning or unusual system behaviour; and
c. cooperate with the IT Department during malware investigation and remediation.

8.2 Employees shall not:

a. disable, uninstall, or modify antivirus or endpoint protection software;
b. ignore malware warnings or security alerts; or
c. attempt to remove malware without informing the IT Department.

9. Email Security

Electronic mail remains one of the principal methods by which cybercriminals attempt to compromise information systems. All users shall therefore exercise due diligence while using official email services.

9.1 Employees shall:

a. carefully examine the sender's identity before opening any email;
b. verify unexpected or suspicious communications through an independent means of communication before acting upon them;
c. inspect hyperlinks before clicking by confirming the destination address;
d. open email attachments only when received from trusted and verified sources;
e. report phishing emails, spam, impersonation attempts, fraudulent communications, or suspicious attachments immediately to the IT Department; and
f. use official email accounts for official correspondence wherever required.

9.2 Employees shall not:

a. respond to emails requesting passwords, banking credentials, One-Time Passwords (OTPs), confidential information, or other sensitive data;
b. click links received from unknown or suspicious sources;
c. download attachments that appear unusual or unexpected without verification;
d. forward phishing or malicious emails to other users except for reporting purposes; or
e. use unofficial email accounts for transmitting confidential School information without prior authorization.

The IT Department may implement email filtering, spam protection, malware scanning, attachment controls, and domain authentication technologies to strengthen email security.

10. Internet Usage

Access to the internet using School resources shall be undertaken responsibly and solely for legitimate educational, administrative, and official purposes.

10.1 Employees shall:

a. access websites only through secure HTTPS connections wherever available;

b. verify the authenticity and security of websites before entering confidential or sensitive information;

c. exercise caution while opening links received through email, SMS, messaging applications, QR codes, or social media platforms;

d. immediately discontinue access to any website that appears suspicious or displays abnormal behaviour; and

e. comply with all applicable copyright, intellectual property, and information technology laws while using internet resources.

10.2 Employees shall not:

a. visit websites known to distribute malicious software or engage in fraudulent activities;

b. download pirated, cracked, or unauthorized software;

c. install browser extensions or plugins that have not been approved by the IT Department;

d. use URL-shortening services or shortened web links unless the authenticity of the destination has been verified;

e. intentionally bypass internet security controls established by the School; or

f. engage in activities that may expose the School's information systems to cyber threats.

The School reserves the right to monitor internet usage on official devices in accordance with applicable laws and institutional requirements.

11. Wi-Fi and Network Security

The security of wireless networks is essential to safeguarding School information and digital infrastructure.

11.1 Employees shall:

a. connect official devices only to authorized and secure wireless networks;

b. verify the identity of wireless networks before connecting;

c. immediately disconnect from any wireless network suspected of being fraudulent or insecure; and

d. report any suspected unauthorized wireless access point to the IT Department.

11.2 Employees shall not:

a. access confidential School information using public Wi-Fi networks unless protected through an approved Virtual Private Network (VPN);

b. connect official devices to unsecured or unknown wireless networks;

c. create unauthorized wireless hotspots using official devices;

d. share School Wi-Fi passwords without authorization; or

e. install unauthorized networking equipment within School premises.

The IT Department shall periodically review wireless network configurations and implement appropriate encryption and authentication mechanisms.

12. Data Protection and Information Security

The School recognizes that information constitutes a valuable institutional asset requiring appropriate safeguards throughout its lifecycle.

Accordingly:

a. confidential information shall be classified and handled according to its level of sensitivity;

b. sensitive information shall be encrypted during storage and electronic transmission wherever technically feasible;

c. access to confidential information shall be granted strictly on a need-to-know basis;

d. confidential information shall be stored only in approved locations and systems;

e. appropriate backup procedures shall be implemented to ensure data availability and recovery;

f. printed confidential records shall be securely stored in locked cabinets or other controlled environments when not in use; and

g. confidential records shall be securely destroyed in accordance with the School's document retention and disposal procedures.

Employees shall not:

a. copy confidential information onto unauthorized storage devices;

b. disclose confidential information to unauthorized persons;

c. retain confidential information beyond the period required for official purposes; or

d. remove confidential documents from School premises without proper authorization.

All users shall ensure that personal information relating to students, parents, employees, and other stakeholders is processed responsibly and only for legitimate educational or administrative purposes.

13. Physical Security of Information Systems

The physical protection of information technology assets is an essential component of the School's cyber security framework. Every employee entrusted with the use of official devices shall exercise reasonable care to prevent unauthorized access, theft, loss, or damage.

13.1 Employees shall:

a. lock or password-protect their computers whenever leaving their workstations unattended, irrespective of the duration of absence;

b. log off from all official applications and systems upon completion of work or before leaving the workplace;

c. ensure that laptops, mobile devices, removable storage media, and other portable equipment remain under their personal control while in use;

d. store official devices in secure locations when not in use;

e. immediately report the loss, theft, or suspected compromise of any official device or storage media to the IT Department and the School Administration; and

f. ensure that confidential documents displayed on computer screens are not visible to unauthorized persons.

13.2 Employees shall not:

a. leave official devices unattended in public places or unsecured areas;

b. permit unauthorized persons to use official devices;
c. disable screen-lock mechanisms or other physical security controls;
d. remove official equipment from School premises without prior authorization; or
e. expose official devices to conditions likely to cause physical damage or data loss.

The IT Department may implement physical access controls, surveillance measures, device tracking mechanisms, and asset management procedures to safeguard School-owned equipment.

14. Use of Official Devices

Official devices are provided exclusively for legitimate educational, administrative, and institutional purposes. Users shall exercise due diligence while using such devices and shall ensure compliance with all applicable School policies.

14.1 Employees shall:

a. use official devices only for authorized purposes;
b. operate devices using standard user accounts unless elevated privileges are expressly authorized;
c. comply with all security instructions issued by the IT Department;
d. maintain the security and confidentiality of data stored on official devices;
e. immediately report any malfunction, suspected compromise, or unauthorized access; and
f. permit periodic inspection, maintenance, security audits, and software updates as directed by the IT Department.

14.2 Employees shall not:

a. install unauthorized software, applications, utilities, or browser extensions;
b. install cracked, pirated, or illegally licensed software;
c. install or use unauthorized remote-access software, including but not limited to TeamViewer, AnyDesk, Ammyy Admin, UltraViewer, or similar applications, without written approval from the IT Department;
d. alter system security configurations without authorization;
e. connect unknown or unauthorized USB storage devices or external hardware to official devices;
f. disable firewall, antivirus, encryption, or other security controls; or
g. use official devices for activities that may expose the School to legal, financial, or cyber security risks.

The School reserves the right to monitor, inspect, and audit official devices to ensure compliance with this Policy, subject to applicable laws.

15. Mobile Applications

The installation and use of mobile applications on official devices shall be restricted to applications that are necessary for legitimate educational or administrative purposes.

15.1 Employees shall:

a. download applications only from official and trusted application stores;
b. install applications only where there is a legitimate operational requirement;
c. ensure that installed applications are updated regularly; and
d. review application permissions before granting access to device resources.

15.2 Employees shall not:

a. install applications obtained from unofficial or unknown sources;

b. use third-party document scanning applications for official documents unless expressly approved by the IT Department;

c. upload official documents to external websites for file conversion, compression, editing, translation, or similar processing without authorization;

d. grant unnecessary permissions to mobile applications that may compromise confidential information; or

e. use applications that are known to present significant cyber security risks.

Where necessary, the School may implement Mobile Device Management (MDM) or other security controls to protect institutional information accessed through mobile devices.

16. Social Media Usage

Employees shall exercise professionalism, integrity, and discretion while using social media platforms, particularly where such use may affect the reputation, security, or interests of the School.

16.1 Employees shall:

a. verify the authenticity of information before sharing or forwarding it;

b. respect confidentiality obligations while using social media;

c. maintain appropriate professional conduct in online communications relating to the School; and

d. immediately report any fake social media account, impersonation, or cyber abuse involving the School to the Management.

16.2 Employees shall not:

a. publish or disclose confidential School information;

b. share student records, employee information, examination materials, financial information, or other confidential data without authorization;

c. circulate unverified news, rumours, or misleading information relating to the School;

d. click suspicious links received through social media platforms;

e. engage in online conduct that may expose the School to cyber security risks or reputational harm; or

f. represent personal opinions as official statements of the School without proper authorization.

Nothing contained herein shall prevent employees from exercising lawful rights, provided that confidential information and institutional interests remain adequately protected.

17. Protection of Sensitive Information

All confidential and sensitive information shall be handled with the highest standards of care to prevent unauthorized disclosure, alteration, or misuse.

17.1 Employees shall not:

a. transmit confidential information through personal messaging applications unless specifically authorized and appropriately secured;

b. disclose passwords, login credentials, authentication codes, or encryption keys;

c. send confidential information over unsecured communication channels;

d. store confidential School information on personal cloud storage services without authorization;

e. disclose confidential information to persons who do not have a legitimate need to know; or

f. leave confidential records unattended in locations accessible to unauthorized persons.

Where electronic transmission of confidential information is unavoidable, appropriate encryption and secure communication methods shall be employed.

The principle of "least privilege" shall govern access to confidential information, ensuring that users receive only such access as is necessary for the performance of their official duties.

18. Printer and Peripheral Security

Network printers, scanners, photocopiers, and other peripheral devices shall be configured and used in a secure manner to prevent unauthorized access to confidential information.

18.1 Employees shall:

a. collect printed confidential documents immediately after printing;

b. verify the intended recipient before scanning or transmitting documents electronically;

c. ensure that confidential documents are not left unattended on printers, photocopiers, or scanners; and

d. report any suspected security issue involving peripheral devices to the IT Department.

18.2 Employees shall not:

a. connect printers or other network peripherals directly to the internet unless expressly authorized by the IT Department;

b. modify printer or scanner configurations without authorization;

c. use personal peripheral devices for official confidential work without approval; or

d. dispose of printed confidential documents except through approved secure disposal procedures.

The IT Department shall ensure that network-connected peripheral devices are configured in accordance with established cyber security standards and are periodically reviewed for security vulnerabilities.

19. Cyber Security Incident Reporting and Response

The timely reporting and effective management of cyber security incidents are essential to minimizing operational disruption, protecting institutional information, and ensuring compliance with applicable legal and regulatory requirements.

Every employee shall immediately report any actual, suspected, or attempted cyber security incident upon becoming aware of the same.

19.1 Cyber security incidents include, but are not limited to:

a. malware or ransomware infections;

b. phishing or spear-phishing attempts;

c. unauthorized access to School systems or accounts;

d. suspected compromise of passwords or user credentials;

e. data leakage, data breach, or unauthorized disclosure of confidential information;

f. theft, loss, or damage of official devices or storage media;

g. denial-of-service attacks;

h. unauthorized modification or deletion of information;

i. suspicious system behaviour or abnormal network activity; and

j. any other event that may compromise the confidentiality, integrity, or availability of the School's information assets.

19.2 Every incident shall be reported without undue delay to:

- the Information Technology (IT) Department;
- the Technical Supervisor;
- the Administrative Officer;
- the Principal; and
- the Manager.

19.3 Upon receipt of a report, the IT Department shall:

a. acknowledge the incident;

b. assess its severity and potential impact;

c. take immediate steps to contain the threat;

d. preserve relevant digital evidence;

e. investigate the incident;

f. recommend appropriate remedial measures;

g. restore affected systems where feasible; and

h. submit an incident report to the School Management.

Employees shall fully cooperate during any cyber security investigation and shall preserve all relevant information, devices, records, and communications relating to the incident.

No employee shall intentionally conceal, delay, interfere with, or destroy evidence relating to a cyber security incident.

20. User Responsibilities

Every user of the School's information systems shares responsibility for maintaining a secure digital environment.

Accordingly, every employee shall:

a. comply with the provisions of this Policy and all related information security procedures;

b. exercise reasonable care while handling confidential information;

c. protect passwords, authentication credentials, and official devices from unauthorized access;

d. immediately report any cyber security incident or suspected vulnerability;

e. participate in cyber security awareness programmes organized by the School;

f. cooperate during cyber security audits, inspections, investigations, and compliance reviews;

g. follow instructions issued by the IT Department regarding cyber security controls;

h. use School ICT resources responsibly and only for legitimate educational or administrative purposes; and

i. contribute towards maintaining a secure and cyber-resilient working environment.

Supervisory personnel shall additionally ensure that employees under their supervision understand and comply with the requirements of this Policy.

21. Prohibited Activities

Without prejudice to any other provision of this Policy, the following activities are strictly prohibited unless expressly authorized in writing by the School:

a. sharing passwords or authentication credentials;
b. using public Wi-Fi networks for official work without an approved secure connection;
c. responding to phishing emails or fraudulent communications;
d. installing unauthorized software or applications;
e. installing cracked or pirated software;
f. disabling antivirus, firewall, encryption, or other security controls;
g. connecting unauthorized USB devices or removable storage media;
h. installing or using unauthorized remote desktop or remote access software;
i. using unofficial document scanning, file conversion, or cloud storage services for official documents;
j. ignoring malware warnings or security alerts;
k. opening suspicious links, QR codes, or email attachments;
l. storing passwords insecurely;
m. leaving computers or mobile devices unlocked or unattended;
n. publishing confidential School information through social media or any other public platform;
o. accessing websites through unverified SMS, messaging applications, or shortened links without appropriate verification;
p. attempting to bypass security controls implemented by the School;
q. engaging in any activity that may expose the School to cyber security threats or legal liability; and
r. knowingly assisting or facilitating any unauthorized access to School information systems.

Any prohibited activity may result in immediate disciplinary action irrespective of whether actual loss or damage has occurred.

22. Cyber Security Awareness and Training

The School recognizes that cyber security is a shared responsibility requiring continuous education and awareness.

Accordingly, the School shall periodically organize cyber security awareness programmes for all employees covering, inter alia:

a. password management;
b. phishing awareness;
c. ransomware prevention;
d. safe internet practices;
e. data protection obligations;
f. social engineering attacks;
g. mobile device security;

h. cloud security;
i. cyber incident reporting procedures; and
j. emerging cyber threats.

Employees shall actively participate in such programmes and implement the knowledge acquired in their day-to-day responsibilities.

The School may conduct periodic simulated phishing exercises, security assessments, or awareness campaigns to evaluate compliance and improve cyber resilience.

23. Monitoring, Audit, and Compliance

To safeguard its information assets and ensure compliance with this Policy, the School reserves the right, subject to applicable law, to monitor, inspect, audit, and review the use of its information systems, devices, networks, and digital resources.

Such monitoring may include:

a. system logs;
b. network activity;
c. internet usage;
d. email security logs;
e. software installations;
f. endpoint security reports;
g. access records; and
h. other information reasonably necessary to protect the School's information systems.

Employees shall have no expectation of privacy with respect to official systems, except as may be provided under applicable law.

Information obtained through monitoring shall be used solely for legitimate administrative, operational, investigative, compliance, or legal purposes.

Periodic cyber security audits and vulnerability assessments may be conducted to verify compliance with this Policy and to identify opportunities for continuous improvement.

24. Policy Violations and Disciplinary Action

Compliance with this Policy is mandatory.

Any violation of this Policy shall constitute misconduct and may result in disciplinary action commensurate with the nature and gravity of the violation.

Without prejudice to any other legal remedy available to the School, disciplinary measures may include:

a. verbal or written warning;
b. mandatory cyber security retraining;
c. temporary suspension of access to information systems;
d. withdrawal of user privileges;
e. recovery of financial losses or damages caused by negligence or misconduct, where permissible under law;
f. disciplinary proceedings under the applicable service rules;

g. termination of employment or contractual engagement in appropriate cases;
h. reporting the matter to competent governmental or law enforcement authorities where required; and
i. initiation of civil or criminal proceedings, wherever applicable.

The School reserves the right to take any additional action considered necessary to protect its information assets and institutional interests.

25. Review of the Policy

This Policy shall be reviewed at least once every year or earlier whenever considered necessary due to:

a. changes in applicable laws, regulations, or Government directives;
b. recommendations issued by CERT-In, MeitY, the Directorate of Education, or other competent authorities;
c. technological developments;
d. emerging cyber security threats;
e. significant cyber incidents; or
f. operational requirements of the School.

Any amendment or revision shall become effective upon approval by the School Managing Committee.

26. Approval

This Cyber Security Policy has been approved and adopted by the School Managing Committee of Faith Academy at its meeting held on **20 July 2026** and shall come into force with immediate effect unless otherwise specified.

27. Publication and Acknowledgement

This Policy shall be:

a. published on the School's official website;
b. made available in the School Library and Administrative Office;
c. circulated to all employees through official communication channels;
d. explained during induction and periodic cyber security awareness programmes; and
e. acknowledged by every employee, who shall confirm that he or she has read, understood, and agrees to comply with the provisions of this Policy.

Failure to acknowledge receipt of this Policy shall not exempt any employee from compliance with its provisions.

Mr. C. Sundaraj **Director** **Faith Academy Schools & Projects**	**Dr. M. Kannan** **Principal & Manager** **Faith Academy**	E. Robert **Mrs. E. Robert** **Principal & Manager** **Faith Academy Second Shift**

FAITH ACADEMY

STUDENT TRANSPORT SAFETY PROTOCOL

1. Preamble

Faith Academy is a Senior Secondary Unaided Minority Institution in Delhi, established and administered under the protection of Article 30(1) of the Constitution of India. While the School exercises administrative autonomy in its day-to-day functioning, the safety of every child travelling to and from school is treated as a non-negotiable priority. This Protocol sets out the standards, responsibilities, and procedures governing all modes of school-arranged transport, having regard to the Motor Vehicles Act, 1988, the Central Motor Vehicles Rules, 1989, the guidelines of the Hon'ble Supreme Court of India on school bus safety, circulars issued by the CBSE and the Transport Department, Government of NCT of Delhi, and applicable child-protection legislation.

This Protocol applies in addition to, and does not derogate from, the School's Anti-Bullying and Child Protection Policies, which continue to apply to student conduct and staff-student interaction during transit.

2. Objectives

2.1 To ensure that every vehicle used for school transport is roadworthy, appropriately licensed, and fitted with prescribed safety equipment.

2.2 To ensure that drivers, conductors, and attendants engaged in school transport are verified, trained, and of good character.

2.3 To establish clear procedures for boarding, travel, alighting, and emergency response.

2.4 To provide parents with transparency and real-time information regarding their child's transit.

2.5 To fix institutional responsibility through a designated Transport Committee and Transport In-Charge.

2.6 To ensure compliance with applicable statutory and regulatory requirements while respecting the School's autonomy as a minority institution.

3. Applicability and Scope

This Protocol applies to:

3.1 All buses owned, leased, or contracted by the School for the transport of students;

3.2 All students, drivers, conductors/attendants, route supervisors, and parents/guardians availing of school transport;

3.3 Transport arrangements for co-curricular activities, sports events, excursions, and educational tours.

Where a student is transported by a private vehicle/van not registered with or verified by the School, the School's responsibility is limited to information-sharing with parents; such vehicles shall nonetheless be encouraged to meet the standards set out in this Protocol as a matter of child safety.

4. Legal and Regulatory Framework

This Protocol has been framed with reference to, and in the spirit of:

4.1 The Motor Vehicles Act, 1988 and the Central Motor Vehicles Rules, 1989, including provisions relating to permits, fitness certificates, and vehicle specifications for the transport of school children.

4.2 Guidelines of the Hon'ble Supreme Court of India (including directions issued in matters concerning school bus safety) on maximum seating, speed governors, fire extinguishers, first-aid kits, and window grills/guard rails.

4.3 Circulars of the Central Board of Secondary Education on transport safety for affiliated schools.

4.4 Guidelines and permit conditions prescribed by the Transport Department, Government of NCT of Delhi, for school buses/vans plying in Delhi.

4.5 The Protection of Children from Sexual Offences (POCSO) Act, 2012, and the Juvenile Justice (Care and Protection of Children) Act, 2015, insofar as they govern the conduct of adults engaging with children.

4.6 The Right of Children to Free and Compulsory Education Act, 2009, to the extent applicable to the School.

Nothing in this Protocol shall be construed as a waiver of the School's rights and protections available under Article 30(1) of the Constitution; the School adopts these standards voluntarily in the interest of student safety.

5. Vehicle Standards and Fitness

5.1 Registration, Permit and Colour

5.1.1 Every school bus shall be painted the prescribed 'school bus' colour (yellow), bear the words 'SCHOOL BUS' prominently on front and rear, and display the School's name, address, and a valid contact number.

5.1.2 Every vehicle shall hold a valid fitness certificate, a valid contract carriage/school bus permit, valid insurance (including passenger liability cover), and a valid Pollution Under Control certificate, all renewed as per statutory timelines.

5.2 Safety Fittings

5.2.1 Speed governor limiting speed to the prescribed maximum (ordinarily 40 km/h, or as prescribed by the Transport Department) fitted and sealed.

5.2.2 First-aid box, fire extinguisher (functional and within validity), and a fire-safety exit/emergency window as prescribed.

5.2.3 Horizontal grills/guard rails on windows, and a functional public address arrangement where the bus capacity so requires.

5.2.4 GPS tracking device linked to the School's transport monitoring system and, where feasible, to a parent-facing tracking app.

5.2.5 CCTV camera(s) covering the passenger cabin, with recordings retained for a minimum period as prescribed by the Management.

5.2.6 Seating strictly within the certified capacity of the vehicle; standees are not permitted.

5.3 Inspection and Maintenance

5.3.1 Every vehicle shall undergo a documented daily pre-trip check (brakes, tyres, doors, lights, fuel, first-aid kit, fire extinguisher) by the driver, verified periodically by the Transport In-Charge.

5.3.2 A comprehensive mechanical inspection shall be conducted at least once every term by an authorised service provider.

6. Drivers, Conductors and Attendants

6.1 Eligibility and Verification

6.1.1 Drivers shall hold a valid heavy/light motor vehicle driving licence (as applicable) with a minimum of five years' driving experience and a Badge issued by the Transport Department for driving school vehicles, where prescribed.

6.1.2 Police verification/character certificate shall be obtained and kept current for every driver, conductor, and attendant prior to engagement, and renewed periodically.

6.1.3 Drivers and conductors shall not have any record of traffic offences involving rash or negligent driving, drunken driving, or offences against children.

6.1.4 At least one attendant shall be present on every bus in addition to the driver, responsible for boarding/alighting supervision and student discipline en route.

6.2 Training and Conduct

6.2.1 Drivers and attendants shall undergo induction training covering safe driving practices, child safety, emergency/first-aid response, and appropriate conduct with minors, followed by periodic refresher training.

6.2.2 Use of mobile phones while driving, consumption of alcohol/tobacco on duty, and smoking inside the vehicle are strictly prohibited.

6.2.3 Drivers and attendants shall not administer any form of physical or verbal discipline to a student; any concern regarding student behaviour shall be reported to the Class Teacher/Transport In-Charge.

6.2.4 Attendants shall not be left alone with an individual child in circumstances that depart from the ordinary group transit setting.

7. Route Planning and Scheduling

7.1 Routes shall be planned by the Transport In-charge having regard to road conditions, traffic density, and reasonable travel time, and reviewed at the start of each academic session and whenever a significant change in enrolment or address occurs.

7.2 Each route shall have a designated list of boarding/alighting points, communicated in writing to parents, with pickup/drop timings indicated as approximate and subject to traffic.

7.3 A Route Chart, Attendant's Manifest (list of students with class, section, and pickup/drop point), and Emergency Contact List shall be maintained on every vehicle at all times.

7.3 No unauthorised stoppage, detour, or pickup/drop of any person not on the manifest shall be permitted.

8. Boarding, Travel and Alighting Protocol

8.1 The attendant shall physically verify each child's identity against the manifest at the time of boarding and alighting.

8.2 A child shall be handed over at the drop point only to the parent/guardian or an authorised person recorded with the School, unless the parent has provided written consent for the child to walk home independently from a fixed point.

8.3 If no authorised person is present to receive a child at the drop point, the child shall not be left unattended; the attendant shall contact the parent and, if necessary, return the child to school or to a designated safe point, as per the School's standing instructions.

8.4 The bus shall not move until all students are seated (or safely seated with seatbelts where fitted) and the entry/exit doors are secured.

8.5 The attendant shall conduct a physical head-count and a final walk-through of the vehicle at the end of every trip before the vehicle is parked, to ensure no child is left on board.

8.6 Students shall not be permitted to put any part of the body outside the window, and shall remain seated for the duration of the journey.

9. Emergency Response and Breakdown Procedure

9.1 In the event of a breakdown, accident, or medical emergency, the driver/attendant shall immediately inform the Transport In-Charge and follow the School's emergency contact protocol, while ensuring students remain within the vehicle or move to a safe location as circumstances require.

9.2 In case of an accident, the School shall promptly inform parents of affected students, arrange first aid/medical attention, and cooperate with the police and insurance authorities as required by law.

9.3 During adverse weather (fog, heavy rain, waterlogging) or poor visibility, routes may be modified, timings adjusted, or trips suspended on the directions of the Principal/Transport Committee, with prior communication to parents wherever feasible.

10. Reporting and Grievance Redressal

Any parent, student, or staff member may report a transport-related safety concern (e.g., overspeeding, unsafe driving, unauthorised stoppage, staff conduct, vehicle condition) to the Transport In-Charge or through the School's designated complaint channel/helpline. Complaints shall be acknowledged within 24 hours and, save in exceptional circumstances, resolved or substantively responded to within 7 working days. Complaints involving suspected misconduct with a child shall be immediately escalated to the Anti-Bullying/Child Protection Committee and dealt with under the School's Child Protection Policy, including mandatory reporting under the POCSO Act, 2012, where applicable.

11. Responsibilities of Parents/Guardians

11.1 Ensure the child reaches the designated boarding point on time; the vehicle shall not wait beyond a reasonable period at any stop.

11.2 Keep the School informed of any change in address, pickup/drop point, or authorised person for receiving the child.

11.3 Promptly report any safety concern observed during transit.

11.4 Ensure that a responsible adult is available to receive the child at the drop point, or provide written consent where the child is permitted to proceed independently.

12. Review of the Protocol

This Protocol shall be reviewed by the Management/School Management Committee at least once every academic year, or earlier if warranted by regulatory changes, incidents, or feedback from stakeholders. Suggestions for improvement may be submitted by any stakeholder to the Transport Committee.

13. Declaration

This Protocol has been adopted by the School Management Committee on 20.07.2026, in exercise of its administrative autonomy as an Unaided Christian Minority Institution, and reflects its unwavering commitment to the safety of every child availing of school transport.

Mr. C. Sundaraj **Director** **Faith Academy Schools & Projects**	**Dr. M. Kannan** **Principal & Manager** **Faith Academy**	E. Robert **Mrs. E. Robert** **Principal & Manager** **Faith Academy Second Shift**

Annexure A: Daily Pre-Trip Vehicle Check Form

Vehicle No. / Route No.	
Date	
Brakes, Steering, Tyres Checked (Y/N)	
Lights, Indicators, Horn Working (Y/N)	
Fire Extinguisher in Place & Valid (Y/N)	
First-Aid Box Stocked (Y/N)	
Speed Governor Seal Intact (Y/N)	
GPS & CCTV Functional (Y/N)	
Doors & Window Grills Secure (Y/N)	
Driver's Licence/Badge Displayed (Y/N)	
Remarks	
Checked By (Driver) — Signature	
Verified By (Transport In-Charge) — Signature	

Annexure B: Route Manifest (Illustrative Format)

S.No.	Student Name	Class/Sec	Pickup Time	Pickup / Drop Point
1				
2				
3				

Note: A completed manifest, along with the Emergency Contact List and Route Chart, shall be carried on board every vehicle at all times.

FAITH ACADEMY

STUDENT DISCIPLINE POLICY

1. Philosophy and Purpose

Faith Academy is committed to fostering a safe, respectful, and Christ-centered learning environment where students grow academically, socially, and spiritually. Discipline at Faith Academy is rooted in the belief that correction should be redemptive rather than purely punitive — guiding students toward maturity, personal responsibility, and restored relationships, consistent with our school's mission and values.

This policy applies to all students during school hours, on school property, at school-sponsored events, on school transportation, and in any online conduct that substantially disrupts the school environment or violates school values.

2. Guiding Principles

2.1 Grace and Accountability — Every disciplinary response balances compassion with the need for students to take ownership of their actions.
2.2 Consistency and Fairness — Rules apply equally to all students regardless of background, grade level, or academic standing.
2.3 Restoration — Where possible, discipline aims to repair harm and restore relationships between students, staff, and the school community.
2.4 Communication — Parents/guardians are partners in the disciplinary process and will be informed promptly of significant concerns.
2.5 Developmental Appropriateness — Consequences are calibrated to the student's age, maturity, and history of behavior.

3. Expected Conduct

Students are expected to:

3.1 Treat faculty, staff, and peers with honesty, kindness, and respect
3.2 Follow classroom and campus rules established by teachers and administration
3.3 Take responsibility for their own learning and behavior
3.4 Dress and speak in a manner consistent with the school's community standards
3.5 Refrain from behavior that endangers the safety or wellbeing of others

4. Classification of Offenses

Level 1 — Minor Infractions

Examples: dress code violations, minor disruption, tardiness, incomplete homework, minor disrespect.

Typical Response

a. Verbal warning/redirection by teacher
b. Reflection conversation or written reflection
c. Loss of privilege (e.g., recess, free time)
d. Teacher-parent communication

Level 2 — Moderate Infractions

Examples: repeated Level 1 behavior, cheating/academic dishonesty, disrespect toward staff, minor physical conflict, unauthorized use of electronic devices, inappropriate language.

Typical Response

a. Office referral
b. Parent conference
c. Detention or in-school reflection time
d. Behavior contract or improvement plan
e. Temporary loss of privileges (e.g., extracurricular participation)

Level 3 — Serious Infractions

Examples: bullying or harassment, fighting, defiance of authority, theft, vandalism, possession of prohibited items (e.g., tobacco, vaping devices), plagiarism on major assignments.

Typical Response

a. Administrative investigation
b. In-school or out-of-school suspension (typically 1–3 days)
c. Mandatory parent meeting
d. Restorative conference with affected parties
e. Probationary status

Level 4 — Severe Infractions

Examples: violence causing injury, possession of weapons, possession or use of illegal substances, threats of harm, hate speech or discriminatory harassment, sexual misconduct, repeated Level 3 violations.

Typical Response

a. Immediate removal from classroom/campus
b. Out-of-school suspension (typically 3–10 days) pending investigation
c. Mandatory involvement of school leadership and, where required by law, local authorities
d. Possible expulsion following formal review
e. Referral to counseling or external support services as appropriate

> *Note: Any conduct involving weapons, threats of violence, or suspected abuse will be reported to appropriate legal authorities in accordance with applicable law, regardless of internal disciplinary outcome.*

5. Disciplinary Procedures

5.1 Investigation — Staff or administration will gather facts from all involved parties before determining consequences.
5.2 Documentation — All Level 2 and above incidents are documented in the student's disciplinary record.
5.3 Parent Notification — Parents/guardians will be notified of Level 2+ incidents within 24 hours (or immediately for Level 3–4).

5.4 Right to Respond — Students and parents have the right to share their perspective before final consequences are determined, except where immediate safety requires urgent action.
5.5 Appeals — Parents may request review of a disciplinary decision by submitting a written appeal to the Head of School within 5 school days.

6. Suspension and Expulsion

In-School Suspension (ISS)

Student remains on campus in a supervised setting separate from regular classes.

Out-of-School Suspension (OSS)

Student is removed from campus for a defined period; missed academic work may be made up per teacher discretion.

Expulsion

Reserved for the most severe or repeated serious violations, determined through a formal review involving the Head of School, relevant staff, and (where applicable) the school board. Parents will be given written notice of grounds and process.

7. Restorative Practices

Where appropriate, Faith Academy incorporates restorative approaches alongside or instead of traditional consequences, including:

a. Guided conversations between affected students
b. Mediated apologies and reconciliation meetings
c. Service or restitution to repair harm done
d. Mentorship or counseling support

8. Anti-Bullying and Harassment

Faith Academy maintains zero tolerance for bullying, cyberbullying, and harassment of any kind. Reports may be made confidentially to any staff member or administrator. All reports will be promptly investigated, and appropriate consequences (up to and including suspension or expulsion) will be applied based on severity.

9. Roles and Responsibilities

9.1 Teachers — Address minor issues directly; refer moderate/serious issues to administration; document incidents.
9.2 Administration — Investigate referred incidents, determine consequences for Level 2+, communicate with parents, maintain records.
9.3 Parents/Guardians — Support the school's discipline policy at home, attend required conferences, communicate concerns constructively.
9.4 Students — Understand and follow school expectations; take responsibility for their choices.

10. Policy Review

This policy will be reviewed annually by school administration and updated as needed to reflect best practices, legal requirements, and community feedback.

This document is intended as a template. Faith Academy should have this policy reviewed by legal counsel familiar with applicable state/local education law before adoption, particularly regarding suspension/expulsion procedures, due process rights, and reporting obligations for minors.

Mr. C. Sundaraj
Director
Faith Academy Schools & Projects

Dr. M. Kannan
Principal & Manager
Faith Academy

E. Robert
Mrs. E. Robert
Principal & Manager
Faith Academy Second Shift

FAITH ACADEMY

ANTI-DRUG AND ANTI-TOBACCO POLICY

1. Preamble

Faith Academy is committed to providing a safe, healthy and nurturing environment for the holistic development of every student. The use, possession, sale or promotion of tobacco, drugs, alcohol and other intoxicating or psychoactive substances poses a serious threat to the physical, mental and social well-being of children and young people.

This policy has been framed in line with the guidelines issued by the Ministry of Education, the National Commission for Protection of Child Rights (NCPCR), the Central Board of Secondary Education (CBSE)/affiliating board circulars, the Cigarettes and Other Tobacco Products Act, 2003 (COTPA), the Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985, and the Juvenile Justice (Care and Protection of Children) Act, 2015, as applicable, to establish a tobacco-free and drug-free educational institution.

2. Objectives

2.1 To create and maintain a 100% tobacco-free, alcohol-free and drug-free campus.
2.2 To protect students, staff and visitors from exposure to tobacco smoke, drugs and other intoxicants.
2.3 To build awareness among students, parents and staff on the health, legal and social consequences of substance use.
2.4 To establish clear, fair and consistent procedures for prevention, reporting, intervention and disciplinary action.
2.5 To ensure compliance with all applicable national and local laws relating to tobacco and narcotic substances.
2.6 To provide counselling, support and rehabilitation pathways rather than purely punitive measures, wherever appropriate.

3. Scope and Applicability

This policy applies to:

3.1 All students enrolled at Faith Academy, at all grade levels.
3.2 All teaching and non-teaching staff, including contractual and outsourced personnel.
3.3 Vendors, contractors, transport staff, canteen operators and visitors on campus.
3.4 All school premises, buildings, playgrounds, transport vehicles, hostels (if any) and school-organised events, excursions, and activities conducted off-campus.

A radius of 100 yards (approximately 91 metres) around the school premises is designated a "Tobacco-Free Area" in accordance with COTPA guidelines, and the sale of tobacco products within this radius is strictly prohibited.

4. Definitions

4.1 "Tobacco Products" — cigarettes, bidis, cigars, gutkha, khaini, pan masala containing tobacco, e-cigarettes, vapes, hookah, and any other smoking or smokeless tobacco product.
4.2 "Drugs/Narcotic Substances" — any substance covered under the NDPS Act, 1985, including cannabis, opioids, cocaine, amphetamines and other psychotropic substances, as well as the misuse of prescription or over-the-counter medication.
4.3 "Alcohol" — any beverage containing ethyl alcohol intended for human consumption.
4.4 "Possession" — having a prohibited substance on one's person, in a bag, locker, vehicle or any other space under one's control.
4.5 "Campus" — all land, buildings and vehicles owned, leased or operated by the school, and any venue hosting a school-sanctioned event.

5. Prohibited Conduct

The following are strictly prohibited on campus, on school transport, and at all school-sponsored events, regardless of the time of day:

5.1 Smoking, chewing, vaping or otherwise consuming any tobacco product.
5.2 Possessing, distributing, selling, or offering for sale any tobacco product, drug, narcotic substance or alcohol.
5.3 Being under the influence of alcohol, drugs or any intoxicating substance.
5.4 Possessing drug paraphernalia (e.g., rolling papers, vape devices, syringes not prescribed for medical use).
5.5 Advertising, sponsorship or promotion of tobacco or alcohol products, including branded merchandise, within school premises or publications.
5.6 Coercing, encouraging or abetting another person, especially a minor, to use tobacco, drugs or alcohol.

6. Roles and Responsibilities of the School and Parents

School Management / Principal

6.1 Displays of "Tobacco-Free Area" signage at all entry points as mandated under COTPA Section 4.
6.2 A Nodal Officer / Tobacco Control Officer to oversee implementation and compliance has been designated.
6.3 This policy is communicated to all stakeholders and reviewed periodically.

Teachers and Staff

6.4 Exhibit tobacco-free and drug-free behaviour at all times on campus.
6.5 Remain vigilant for signs of substance use or distress among students and report concerns promptly.
6.6 Support the delivery of life-skills and awareness education as part of the curriculum.

Students

6.7 Abide by this policy at all times, on campus, on transport and at school events.

6.8 Report any instance of substance use, possession or peer pressure to a teacher, counsellor or the Nodal Officer.

Parents / Guardians

6.9 Reinforce the school's stance on substance use at home and cooperate with school interventions.

6.10 Attend awareness sessions and respond promptly to school communication regarding their ward's conduct.

7. Prevention and Awareness Programmes: The School Shall

7.1 Impart age-appropriate life-skills education, integrated into the curriculum, covering the health risks of tobacco, drugs and alcohol, peer-pressure resistance, and decision-making skills.

7.2 Conduct annual awareness campaigns, workshops, poster/slogan competitions and guest sessions by health professionals, in coordination with the school Health and Wellness programme.

7.3 Conduct sensitisation sessions for parents during orientation and Parent-Teacher meetings.

7.4 Prominently display of "Tobacco-Free Area" and "No Smoking" signage at all entrances, corridors and common areas.

7.5 The staff to recognise early warning signs of substance misuse and respond sensitively.

8. Reporting Procedure

Any student, staff member or parent who becomes aware of a violation of this policy should report it through one of the following channels:

8.1 Directly to the Class Teacher, School Counsellor, or Nodal Officer.

8.2 Through a confidential written note dropped in the designated suggestion/complaint box or email.

All reports will be treated confidentially and investigated fairly. No student or staff member will face retaliation for a good-faith report made under this policy.

9. Disciplinary Framework

Response to a confirmed violation will be graded, age-appropriate, and will prioritise counselling and correction for students, while ensuring accountability. A suggested framework is outlined below; the school's Discipline Committee retains discretion based on the severity and circumstances of each case.

Nature of Violation	First / Minor Instance	Repeat / Serious Instance
Possession or use of tobacco	Counselling, written warning, parent notification	Suspension pending Discipline Committee review; mandatory counselling
Possession or use of drugs/alcohol	Immediate parent notification, counselling referral, written warning	Suspension/expulsion as per Discipline Committee; referral to appropriate authorities/health professionals where required by law
Sale, distribution or supply to others	Not applicable — treated as serious violation on first instance	Expulsion consideration; reporting to parents and, where legally mandated, to authorities

For staff, vendors and visitors, violations will be addressed under the applicable service rules, contractual terms, or visitor code of conduct, and may result in warning, removal from premises, or termination of engagement, as appropriate.

Where a student's conduct may involve a criminal offence under the NDPS Act or COTPA, the school will act in accordance with the Juvenile Justice (Care and Protection of Children) Act, 2015, and applicable law, balancing legal obligations with the best interests of the child.

10. Support, Counselling and Rehabilitation

Faith Academy recognises that substance use among young people is often linked to underlying stress, peer influence, or personal difficulties. Wherever appropriate, disciplinary action will be accompanied by:

10.1 Confidential counselling through the school counsellor.
10.2 Referral to external medical or psychological support services with parental consent.
10.3 A structured re-integration plan for the student following any period of suspension.
10.4 Regular follow-up to monitor the student's well-being and progress.

11. Legal Compliance and Campus Signage

11.1 "Tobacco-Free Area" boards will be displayed at all entrances in accordance with COTPA, 2003 and its Rules.

11.2 No advertisement, sponsorship or promotional material relating to tobacco or alcohol shall be permitted on campus or in school publications.

11.3 Sale of tobacco products to or by anyone under 18 years of age is prohibited under law and under this policy.

11.4 The school canteen and vendors on campus shall not stock, sell or advertise tobacco, drug paraphernalia or alcohol.

12. Monitoring and Review

The Nodal Officer, in coordination with the Discipline Committee and School Counsellor, will monitor compliance with this policy, maintain records of reported incidents (in a confidential manner), and present an annual compliance report to the Principal and School Management Committee.

This policy will be reviewed annually, or earlier if required by changes in law, board circulars, or institutional experience, to ensure it remains effective and relevant.

13. Acknowledgement

All students and parents/guardians are required to sign an acknowledgement of this policy at the time of admission and at the start of each academic year. Staff members will acknowledge the policy as part of their service agreement.

E. Robert

Mr. C. Sundaraj
Director
Faith Academy Schools & Projects

Dr. M. Kannan
Principal & Manager
Faith Academy

Mrs. E. Robert
Principal & Manager
Faith Academy Second Shift