



PUNJAB STATE LEGAL SERVICES AUTHORITY'S CYBER SURAKSHA SCHEME 2026

*Public Awareness Against Cyber-Crimes and Digital Arrest Scams,
and Victim Recovery Assistance*

Adopted in discharge of the functions of the Punjab State Legal Services Authority under
Sections 7 and 8, read with Sections 6, 10, 11, 11B, 12 and 13 of the Legal Services
Authorities Act, 1987, and the applicable rules and regulations.

CHAPTER I — PRELIMINARY

1 Short title, extent and commencement

This Scheme shall be called the “Punjab State Legal Services Authority’s Cyber Suraksha Scheme, 2026”. It shall extend throughout Punjab and take effect on the date specified in PSLSA’s approval and issuance order. Assistance may be sought for earlier incidents where a remedy remains available under law.

2 Definitions

“Act” means the Legal Services Authorities Act, 1987; “PSLSA” means the Punjab State Legal Services Authority; “DLSA” means a District Legal Services Authority in Punjab; and “SDLSC” means the competent Sub-Divisional Legal Services Committee.

“Cyber-crime” includes an offence in which a computer, communication device or digital network is the means or target, including financial fraud, identity theft, online impersonation, cyber-stalking, extortion and misuse of electronic content.

“Digital arrest scam” means a fraud in which a person impersonates a judicial, police, investigative, regulatory or other public authority, including through forged documents, deepfake audio/video or electronic communication, and uses false accusations or threats of detention to induce payment, disclosure of information or other compliance. The expression does not describe a lawful mode of arrest.

“Victim” means a person seeking assistance on the allegation of financial loss, harassment or other injury from cyber-crime; receipt of assistance does not determine the allegation’s merits.

“Unit” means a State or District Cyber Redressal Unit constituted under this Scheme. “Panel lawyer”, “PLV” and “legal services” carry the meanings applicable under the Act and NALSA framework.

“NCRP” means the National Cybercrime Reporting Portal at <https://cybercrime.gov.in>; “1930” means the national cyber-fraud reporting helpline; and “CFCFRMS” means the Citizen Financial Cyber Fraud Reporting and Management System.

3 Objectives and scope

The Scheme shall promote recognition and prevention of cyber-crime; facilitate urgent reporting; provide eligible victims with competent legal assistance; and support applications and follow-up for restoration.

Awareness and initial reporting guidance shall be accessible to all. Particular attention shall be given to digital arrest and financial fraud, without excluding victims of other cyber-crimes from appropriate legal assistance and referral.

4 Eligibility and governing safeguards

No person shall be denied immediate reporting guidance merely for want of an FIR, residence proof, income certificate or complete transaction records. Any Unit approached shall first facilitate urgent action and thereafter arrange a documented referral, if necessary.

Grant of legal aid and representation shall be determined under Sections 12 and 13 of the Act and applicable NALSA regulations. Eligibility under an independent statutory category shall not be made conditional upon satisfying an income test. The competent legal services institution shall decide applications promptly under the governing procedure and communicate rejection, reasons and available review/appeal remedies. This Scheme does not enlarge statutory eligibility.

Persons not eligible for funded representation may, with consent, be referred to willing pro bono advocates, legal services clinics or other lawful assistance. The Unit shall explain the scope of the referral and obtain the receiving provider's acceptance.

The Units facilitate legal services; they do not investigate offences, decide ownership of disputed funds, order account freezes or releases, or guarantee recovery. Their administrative coordination shall not influence adjudication or compromise legal professional confidentiality.

CHAPTER II — INSTITUTIONAL ARRANGEMENTS

5 State Cyber Redressal Unit

PSLSA shall establish a State Cyber Redressal Unit under the supervision of the Member Secretary. It shall comprise a designated PSLSA Nodal Officer as coordinator, an advocate with cyber-law experience designated from the existing panel of advocates empanelled under the National Legal Services Authority (Free and Competent Legal Services) Regulations, 2010 (the "2010 Regulations"), a senior Punjab Police cyber-wing liaison officer nominated by the competent police authority, a technical support person and an assistant responsible for records and follow-up. Existing staff may be designated subject to workload and sanction.

The Unit shall prepare operating materials, maintain an authenticated contact directory, support complex and inter-State referrals, train district teams, monitor implementation and consolidate compliance reports. Police participation shall be for liaison; privileged legal consultations shall

be held separately.

6 District Cyber Redressal Units

The Chairman of each DLSA shall constitute and supervise a District Cyber Redressal Unit. The Secretary, DLSA shall be its operational head and District Nodal Officer. The Unit shall include an advocate designated from the DLSA's existing panel of advocates empanelled under the 2010 Regulations, a cyber-police liaison officer nominated by the competent police authority, and a designated system officer or other suitably trained technical support person. Trained PLVs and a designated record assistant shall support the Unit.

The District Lead Bank Manager, bank nodal officers and an appropriately nominated prosecutor may be invited for coordination or training. They shall not participate in confidential advice to a person whose interests conflict with the institution they represent. Nomination or availability of an external representative shall not delay initial assistance.

Each active matter shall have a named case coordinator and next-action date. The Secretary shall resolve allocation gaps and supervise urgent escalations.

7 State oversight and district coordination

A State Steering and Monitoring Committee, chaired by the Member Secretary, Punjab State Legal Services Authority, shall oversee the Scheme. The Committee shall include such Secretary, District Legal Services Authority, as may be nominated by the Member Secretary. Police, banking, relevant State departments and technical experts may participate through nominations or invitation approved by the competent authorities.

The Committee shall meet quarterly to review performance, resource needs and systemic obstacles. Operational review by the State Unit shall be monthly. Each DLSA shall hold a quarterly stakeholder coordination meeting under its Chairman, with urgent issues escalated between meetings. Committees shall discuss anonymised case patterns unless identifiable information is necessary and lawfully shareable.

8 Access, helplines and outreach points

District Units shall operate through existing front offices and legal services clinics. Sub-Divisional Legal Services Committees and mobile clinics shall facilitate access in remote areas. Assistance shall be available in Punjabi and Hindi, with English and interpretation support as required; reasonable accommodation shall be provided for disability and communication barriers.

PSLSA shall earmark a cyber-assistance contact or extension, and DLSAs shall identify trained staff for their published contact numbers. Verified numbers, office hours and accessible contact methods shall be published. Outside staffed hours, recorded or written guidance shall prominently direct financial-fraud victims to 1930, NCRP and their bank's official fraud-reporting channel. A round-the-clock PSLSA service shall be advertised only after staffing is sanctioned and operational.

9 Panel lawyers, PLVs and training

PSLSA and the DLSAs shall draw upon the existing panel of advocates already empanelled under the 2010 Regulations, and shall designate from among them advocates having relevant experience in cyber-law or who have completed training under this Scheme, maintain a duty roster and identify substitutes. Designated advocates shall assess remedies, prepare applications, protect limitation periods and provide monthly case-status reports and immediate reports of urgent developments.

PLVs may assist with intake, portal navigation, evidence organisation, accessibility and follow-up under supervision. They shall not offer independent specialist opinions or promise relief. Staff shall never seek a victim's PIN, password, CVV or OTP; the victim shall personally authenticate access through official facilities.

Initial training for designated advocates and staff shall cover scam recognition, victim communication, reporting, preservation of electronic records, the applicable SOP, banking complaints, court applications, eligibility, confidentiality and conflicts. Refresher training shall be quarterly. Judicial training or participation shall be coordinated through the appropriate High Court or judicial training institution.

CHAPTER III — PUBLIC AWARENESS AND PREVENTION

10 Priority audiences and local delivery

The campaign shall reach the general public, particularly senior citizens, pensioners, women, children, persons with disabilities, rural and first-time digital users, Scheduled Castes and Scheduled Tribes, workers and persons with limited literacy. District plans shall address locally observed fraud patterns, including fake employment, overseas recruitment, investment, KYC, courier and family-emergency impersonation frauds.

DLSAs shall work with Panchayats, educational institutions, legal literacy clubs, self-help groups, banks, Sewa Kendras, worker associations, resident groups and community institutions to provide practical sessions in accessible locations.

11 Minimum programme and approved materials

Every DLSA shall organise at least two dedicated cyber-awareness programmes each month, ordinarily including one rural or otherwise underserved location. Existing events may be used if a distinct cyber-awareness session is delivered and separately recorded. PSLSA shall issue an annual calendar and coordinate an annual intensive awareness week.

PSLSA shall approve a concise Punjabi, Hindi and English booklet, first-response card, presentation and audio/video messages. Materials shall be checked for legal accuracy, accessible language and functioning official links before circulation and reviewed quarterly. DLSAs shall use role-play and demonstrations with fictional data, followed by an explanation of reporting and assistance options.

12 Core public messages

Materials shall explain that “digital arrest” is a scam; uniformed video callers, official-looking letters and caller identification do not establish authenticity; and demands to transfer money to a “safe”, “verification” or “investigation” account are warning signs. They shall advise independent verification through publicly listed official contacts and explain that genuine electronic court or agency processes should also be independently verified.

The campaign shall teach safe handling of OTPs, PINs, links, QR codes, remote-access applications and identity documents; the risks of lending accounts or SIMs; and how to recognise deepfake impersonation, fake investments, recovery agents and fraudulent refund fees.

Every programme shall explain immediate reporting to 1930/NCRP and the bank, preservation of available records without delaying reporting, access to DLSA assistance, and the distinction between money put on hold and money actually returned. Public messages shall avoid blaming or shaming victims.

13 Partnerships and evaluation

PSLSA may coordinate approved public-service messaging through radio, television, print, social media and, through competent agencies, telecom channels. Educational authorities may be approached to incorporate cyber-safety learning in suitable activities or curricula. Partnerships

shall not give commercial entities access to victim data or create endorsements of financial products.

DLSAs shall record audience, locality, attendance and materials used, and assess basic learning through short questions on scam recognition and reporting. Photographs shall not expose victim identities or confidential complaints. Outcomes and underserved locations shall inform the next quarter's programme.

CHAPTER IV — VICTIM ASSISTANCE AND RECOVERY

14 Immediate first response

On receiving a report, staff shall first assess whether fraud is continuing, discourage further payments or disclosure, and facilitate immediate contact with 1930 and the bank/payment provider's official fraud channel, together with NCRP reporting. Staff shall record the time of receipt, reporting attempts and acknowledgements. Failed connections shall trigger alternative official reporting channels and follow-up; completion of the application in the prescribed proforma (Annexure A-1) shall not delay action.

Where the device appears compromised, staff shall guide the victim to use a trusted alternative device or independently verified channel to contact the bank. Necessary protective steps shall be coordinated with competent technical personnel. Original records shall be preserved where safe and practicable; the victim shall not be instructed to remain exposed merely to collect evidence.

For non-financial cyber-crime or immediate physical danger, staff shall facilitate the appropriate police or emergency response rather than treating the financial-fraud channel as the exclusive remedy.

15 Complaint registration and evidence support

The Unit shall assist the victim to record, in the proforma prescribed for this purpose (Annexure A-1), the chronology, impersonated authority, suspect identifiers, amounts, payment references and available screenshots, messages, emails and bank records. It shall help obtain NCRP, bank and police acknowledgements and distinguish each from an FIR. Assistance with Zero FIR/e-Zero FIR shall follow applicable law and actual operational availability; a portal complaint shall not be described as automatically constituting an FIR.

If police registration or action is refused or delayed, the panel lawyer shall examine the appropriate statutory escalation and court remedy. Copies of submitted material and a plain-language next-step explanation shall be provided to the victim.

Only necessary copies shall be taken. Any originals received shall be inventoried, acknowledged and returned when no longer required. Electronic evidence shall be preserved with available source and date information; the lawyer shall address applicable evidentiary requirements without placing unnecessary technical demands on the victim at intake.

16 Case assessment and written action plan

An urgent matter shall reach the duty lawyer/Secretary on the day it is received. Within two working days, the Unit shall ordinarily communicate a preliminary action plan identifying pending reporting steps, known fund status, proposed remedy, missing documents, responsible person and next review date. This administrative target does not replace statutory legal-aid procedures or deadlines.

The lawyer shall distinguish reporting and preservation, restoration of identifiable proceeds, banking-service complaints, civil/consumer remedies and any separately available compensation. Forum, jurisdiction, limitation, related proceedings and competing claims shall be checked before filing. Remedies may proceed concurrently where legally permissible; unnecessary exhaustion of an administrative route shall not prejudice urgent judicial relief.

17 Restoration and grievance mechanisms

The Unit shall help the victim use the applicable SOP and authenticated Money Restoration or Grievance Redressal Module, where relevant and accessible, and obtain status from the competent police/bank officer. If a module is unavailable, assistance shall proceed through existing official channels and lawful court procedures, with the operational difficulty escalated to the State Unit.

The lawyer shall identify the applicable restoration process, including eligible interim-custody procedures, release through the competent court, or attachment and restoration under the BNSS. Monetary thresholds, undertakings, approvals, notices, competing claims and jurisdiction shall be checked against the current SOP and binding orders in each case; no simplified route shall be assumed to apply to every complaint.

For court proceedings, the Unit shall help assemble the complaint, transaction trail, available hold/seizure particulars, investigating officer's report, proof of claim and prescribed undertaking or bond. It shall seek early consideration where justified, assist service of the order

and follow up until compliance or a reasoned impediment is recorded. Administrative units shall not dictate hearing dates or judicial outcomes.

18 Fund status, multiple claims and inter-State matters

The case record shall separately identify loss reported, funds traced where confirmed, amount put on hold/seized, release ordered and amount actually credited to the victim. Unknown amounts shall remain “not confirmed”. Funds shall not be counted as recovered merely because a hold or release order exists.

Where funds are insufficient or several victims claim against the same account, the Unit shall place the issue before the competent authority under the applicable procedure and shall not determine priority or distribution itself. Claims by affected account holders shall receive appropriate legal assessment, with separate counsel where interests conflict.

For another State’s police, bank or court, the State Unit shall arrange contact with the competent legal services institution, retain the referral acknowledgement and monitor handover. For High Court or Supreme Court proceedings, assistance shall be routed to the respective legal services committee. Territorial referral shall not postpone urgent reporting.

19 Banking grievances and other remedies

The Unit shall help the victim complain promptly to the bank/payment provider and retain proof. Counsel shall assess applicable customer-liability, refund and grievance rules on the facts; a transfer induced by deception shall not automatically be treated as an unauthorised transaction carrying a guaranteed refund.

Where maintainable, the Unit may assist a complaint under the applicable Reserve Bank–Integrated Ombudsman Scheme through RBI’s Complaint Management System. The currently applicable scheme, prior bank-complaint requirement, filing period and restrictions concerning parallel proceedings shall be checked. Advocates may advise and prepare documents, but filing or representation must comply with the Ombudsman scheme’s restriction on an advocate acting as authorised representative unless personally aggrieved.

Eligible victims may receive representation before the competent criminal/civil court or consumer commission, as appropriate. Settlement or Lok Adalat referral shall be voluntary and legally maintainable; non-compoundable offences shall not be treated as capable of settlement merely under this Scheme. The Unit shall explain costs covered by legal aid and any exclusions before further action.

20 Vulnerable victims and sensitive complaints

Priority shall be given to ongoing fraud, threatened personal safety, imminent limitation, loss of subsistence and victims requiring assistance because of age, disability, illness, language or distress. Home/mobile assistance may be arranged with consent and appropriate staff safeguards. A trusted support person may assist where authorised and appropriate.

Children and victims of sexual exploitation, cyber-stalking or intimate-image abuse shall be referred through the relevant protective and legal services framework. Applicable mandatory reporting duties shall be observed and explained. Staff shall not ask victims to circulate unlawful sexual material; necessary identification and preservation shall be handled through competent authorities. Counselling and health referrals shall complement legal assistance.

21 Follow-up, escalation and closure

For urgent fund-preservation matters, the coordinator shall check action by the next working day and escalate unacknowledged requests to the District Nodal Officer. Active recovery matters shall ordinarily be reviewed weekly; monthly lawyer reports shall not postpone urgent follow-up. The victim shall receive a status update at least fortnightly while active, or earlier on a material development.

Unresolved cross-agency obstacles shall be referred to the State Unit with the chronology, requested action and supporting acknowledgements. All applicable statutory, court and SOP deadlines prevail over these internal targets.

Closure shall state the assistance provided, amounts actually restored, outstanding proceedings, reasons and future remedies. Sending a referral or lodging a complaint alone shall not be recorded as successful recovery. Administrative closure shall not waive substantive rights; the matter may be reopened on relevant new information or developments.

CHAPTER V — COORDINATION, RECORDS AND ACCOUNTABILITY

22 Confidentiality and data management

Each Unit shall maintain a separate cyber-assistance register using a unique case number and a secure case file. Access shall be restricted by role and purpose. Privileged lawyer-client records shall be kept separately from stakeholder coordination material. Personal data shall be collected

and shared only as necessary on an appropriate lawful basis, with informed consent where required and an explanation of any mandatory disclosure.

Full account identifiers and identity documents shall not appear in routine aggregated reports. Shared material shall use approved secure channels. No staff member shall receive recovered funds into a personal or Unit account. Data retention and secure disposal shall follow an approved records schedule and applicable law, including preservation for pending proceedings. Loss, unauthorised access or disclosure shall be reported promptly to the designated PSLSA officer for remedial action and any required notification.

23 Reporting and evaluation

By the seventh working day of each month, each DLSA shall submit to the State Unit a monthly implementation report for the preceding month in the prescribed proforma (Annexure A-2). The State Unit shall check inconsistencies, consolidate results and submit quarterly implementation reports to NALSA, or earlier/as otherwise directed. Court-compliance reports shall follow the authorised filing channel and prescribed deadline.

Reports shall distinguish new and continuing cases, persons and complaints, and monthly and cumulative figures. Recovery totals shall be supported by confirmation and adjusted for duplicates. Evaluation shall cover response times, unresolved delays, access for vulnerable groups, awareness learning and client feedback, as well as activity counts.

Ms. Jagdeep Kaur Virk

Member Secretary (Incharge)

Punjab State Legal Services Authority

ANNEXURE A-1 — APPLICATION FOR ASSISTANCE BY A VICTIM OF CYBER-CRIME OR DIGITAL ARREST SCAM

(To be submitted before the Secretary, District Legal Services Authority — see Clause 15)

Report to 1930, the National Cybercrime Reporting Portal and your bank first; do not delay reporting to complete this form. No officer, advocate or volunteer shall ask for your PIN, password, CVV or OTP.

A. Applicant

1. Name, age and address: _____
2. Safe mobile number: _____ District / Sub-Division: _____
3. Any accessibility, safety or language need: _____

B. Incident

4. Date and time of incident and of its discovery: _____
5. Authority or institution impersonated, and mode of contact: _____
6. Threat of arrest or “digital arrest” made? Yes / No Fraud still continuing? Yes / No
7. Brief description of the incident: _____

8. Suspect particulars known (numbers, UPI IDs, accounts, links): _____

C. Loss and transactions

Date and time	Amount (₹)	Mode of payment	Beneficiary account / UPI ID and transaction reference

9. Total amount lost: ₹ _____ (in words: _____)

D. Reporting already done and evidence

10. 1930 reference / NCRP acknowledgement number and date: _____

11. Bank complaint reference, and FIR / Zero FIR number and date, if any: _____
12. Any amount placed on hold or seized, as intimated (amount and date): _____
13. Evidence available (screenshots, messages, e-mails, statements, receipts, other): _____

E. Assistance sought

14. Legal advice ☐ assistance in reporting ☐ restoration of money ☐ representation before a court or commission ☐ banking grievance ☐ victim compensation ☐ other ☐

F. Declaration

I state that the particulars given above are true to my knowledge and belief, that I have not applied for assistance in respect of the same incident before any other legal services institution except as disclosed, and that I consent to their being shared with the police, the bank or payment provider and the competent court to the extent necessary for assistance under this Scheme. I understand that assistance under this Scheme does not guarantee recovery of the money lost.

Signature or thumb impression: _____ Place and date: _____

For office use — District Legal Services Authority

Case ID and date of receipt: _____ Received by: _____

Urgent? Yes / No Advocate designated from the existing panel: _____

Case coordinator and next-action date: _____

Signature of the Secretary, DLSA: _____

ANNEXURE A-2 — MONTHLY REPORT BY THE DISTRICT LEGAL SERVICES AUTHORITY TO THE PUNJAB STATE LEGAL SERVICES AUTHORITY

(To be submitted by the seventh working day of the following month — see Clause 23)

District: _____ Reporting month and year: _____

Prepared by: _____ Verified by the Secretary, DLSA: _____

Indicator	Current month	Cumulative since commencement
Awareness programmes held, of which in rural or underserved locations	_____	_____
Persons attending, and advocates, PLVs and staff trained	_____	_____
Applications received in Annexure A-1, and unique persons assisted	_____	_____
Digital arrest cases among the applications received	_____	_____
NCRP complaints facilitated, and FIRs or Zero FIRs confirmed	_____	_____
Legal aid granted / rejected / pending decision	_____	_____
Amount reported lost (₹)	_____	_____
Amount confirmed as held or seized (₹)	_____	_____
Amount ordered for release (₹)	_____	_____
Amount actually credited to victims (₹)	_____	_____
Cases closed: full recovery / partial / other reason	_____	_____
Active cases pending, and matters pending over thirty days	_____	_____
Service grievances received / resolved / pending	_____	_____

Count only additions during the month and show pending balances separately. Successive reports of the same hold shall not be added, and one credit shall not be counted under more than one victim. Unconfirmed figures shall be recorded separately, and closure for “other reason” shall not be counted as successful recovery.

Attach a short anonymised narrative identifying first-response delays, obstacles encountered with the police or banks, accessibility gaps, corrective action requested and the officer responsible. Personally

identifying particulars shall be supplied separately, and only where necessary, through approved secure channels.

Signature of the Secretary, DLSA: _____ Place and date: _____