REDDUNE TRAINING CETNER

SAFEGUARD POLICY

THIS PROCEDURE IS CONTROLLED BY THE RED DUNE TRANING CENTRE AND MAY NOT BE AMENDED, REVISED OR ALTERED IN ANY OTHER WAY WITHOUT THE AUTHORIZATION OF THE COMPANY.

THE SIGNATURES BELOW AUTHORISE ALL PAGES OF THIS PROCEDURE FOR USE FROM THE DATE OF APPROVAL SHOWN

Activity	**Prepared by**	**Approved by**
Name	Naimat Ullah Khan	Akram Ullah
Designation	Centre Manager	Centre Head
Signature		
Date	25 Feb, 2023	17 Mar, 2023

REVISION HISTORY

REVISION	**DATE**	**REMARKS**
1	03 Apr, 2024	
2	01 Mar, 2025	

RED DUNE

Safeguard Policy

REDDUNE TRAINING CETNER

Contents

1. Purpose & Commitment

Red Dune Training Centre (Saudi Arabia) affirms a clear and unequivocal commitment to safeguard every learner, visitor, staff member, contractor, and partner who engages with our Centre—on site, online, or at any off-site activity. We operate a **zero-tolerance** stance toward abuse, harassment, bullying, discrimination, exploitation, and any behavior that could cause physical, psychological, or reputational harm. Safeguarding is integral to our learning mission and to the safe, ethical delivery of international HSE qualifications. It is also a core part of our quality, environmental, and occupational health & safety management approach aligned with ISO 9001 (competence, complaints and improvement), ISO 14001 (risk and stakeholder needs) and ISO 45001 (hazard identification, risk control, worker participation).

Our duty of care means we will:

- Design and run learning environments that are safe, inclusive, and respectful for adults of all backgrounds and abilities.
- Identify, assess, and control safeguarding risks in classrooms, workshops, simulated/practical areas, and during off-site activities.
- Provide clear routes to raise concerns, respond promptly and proportionately, and escalate when necessary to relevant authorities or awarding/TVTC channels.
- Ensure staff and contracted personnel are competent, vetted as appropriate to role, and trained to recognise signs of abuse and respond correctly to disclosures.
- Protect personal data and sensitive case information through disciplined document control and “need-to-know” sharing only.
- Learn from incidents, near misses, complaints, and feedback, and use structured corrective and preventive actions to remove root causes and continuously improve.

Leaders at Red Dune model safe and respectful conduct, resource the safeguarding system adequately, and review performance routinely. All staff, including contractors and visiting specialists, are responsible for following this policy, reporting concerns without delay, and participating in required inductions, briefings, and refreshers. We will not tolerate retaliation against anyone who raises a concern in good faith.

We recognise safeguarding includes (but is not limited to): protection from physical or sexual harm, emotional abuse, neglect, bullying/cyberbullying, harassment and discrimination, exploitation (including financial or labour), unsafe environments or practices, and misuse of digital platforms. Our approach balances prevention, early identification, proportionate response, and continuous improvement.

2. Definitions

This policy applies to **all** Red Dune operations and delivery modes in Saudi Arabia and any locations where Red Dune conducts activities or represents itself. It covers:

People

- **Learners** enrolled on any programmes, qualification, short course, assessment, or induction—regardless of employment status, nationality, or language ability.
- **Vulnerable adults,** including individuals who may, at times or permanently, need additional support due to age, disability, health condition, language barriers, isolation, or other social and personal circumstances.
- **Staff** (permanent, temporary, part-time, visiting trainers/assessors), **contractors**, **consultants**, **volunteers**, and **agency personnel** involved in training, assessment, invigilation, administration, facilities, IT, security, or support services.
- **Visitors** and **clients** on our premises or at our events, including awarding/TVTC reviewers, auditors, and employer representatives.

Activities & Delivery Modes

- **On-site** training, examinations, practical exercises, inductions, meetings, and events.
- **Off-site** activities such as client-site training, field visits, simulated/practical assessments, community events, or conferences.
- **Online/remote** classes, assessments (where permitted), tutorials, forums, messaging, file sharing, and any digital interaction using Red Dune systems or approved platforms.
- **Travel and logistics** arranged by or on behalf of Red Dune (e.g., transport to client facilities or assessment venues).
- **Third-party venues** and partner locations where Red Dune delivers or oversees learning/assessment.

Processes & Interfaces

- **Recruitment and onboarding** of staff and contractors, including role-based screening and reference checks.
- **Induction and mandatory training** on safeguarding, behavioural boundaries, disclosure handling, digital safety, and reporting pathways.
- **Reasonable adjustments** and learner support planning for those with declared needs.
- **Incident, concern, and complaint handling,** including confidential reporting, timely acknowledgement, proportionate investigation, and secure recordkeeping.
- **Information management** (collection, access, retention, and disposal of safeguarding records) under controlled document procedures.
- **Risk assessment and controls** for classrooms, practical spaces, equipment, lone working, mixed-gender environments as applicable, off-site visits, and digital platforms.
- **Contractor and partner management,** ensuring safeguarding expectations are embedded into agreements, inductions, and supervision.

3. Code of Conduct (Staff & Learners)

Purpose
To set clear standards of behaviour that protect learners, staff, contractors, and visitors, and promote a safe, respectful learning environment at Red Dune Training Centre (Saudi Arabia). The Code supports TVTC expectations and the ISO 9001/14001/45001 principles of competence, risk prevention, and continual improvement.

1) Professional boundaries

- Staff maintain appropriate, transparent relationships with learners: no favouritism, secrecy, or conduct that could be misinterpreted as grooming or exploitation.
- Communications, feedback, and one-to-one support are conducted in approved spaces or platforms and, where feasible, within view of others. Doors remain open or windows unobstructed during private meetings.
- Staff do not transport learners in private vehicles or meet off-site without prior written approval from the Centre Manager.
- Personal disclosures are handled sensitively; staff avoid sharing unnecessary personal information and immediately escalate safeguarding concerns to the Designated Safeguarding Lead (DSL).
- Physical contact is avoided unless essential for safety (e.g., first aid). When necessary, it must be proportionate, recorded, and reported.

2) Respectful behavior

- All individuals are treated with dignity, regardless of nationality, language, faith, age, gender, or disability.
- Bullying, harassment, discrimination, retaliation, or degrading language is prohibited.
- Classrooms and workshops must be psychologically safe: disagreements are managed constructively; assessments are invigilated without intimidation.
- HSE expectations are part of respect: follow signage, PPE rules, emergency procedures, and accessible learning arrangements.

3) Use of social media and messaging

- Staff and learners use official, approved channels for teaching, assessment, and results (e.g., Centre email/LMS). Private accounts are not used to discuss Centre matters.
- Messaging groups (e.g., class WhatsApp) require Centre Manager approval, a named staff moderator, and published rules (hours, purpose, no private messaging with individual learners).
- No sharing of learner images, assessments, or personal data on social media. Recording in class requires prior consent and an academic purpose.
- Staff must not “friend” or “follow” learners on personal accounts while the learning relationship exists.
- Any online content that risks reputational harm, exam security, or learner safety must be reported to the DSL.

4) Gifts and conflicts of interest

- Staff do not solicit or accept gifts, cash, favors, or hospitality from learners or suppliers that could influence decisions. Low-value, occasional tokens must be declared to Admin for the gifts register.
- Assessors, invigilators, and IQAs must declare conflicts (e.g., family/financial ties) and be re-assigned if objectivity is at risk.
- Staff do not sell personal services or materials to learners. All fees are paid through official centre channels only.

4. Safer Recruitment

Purpose
To ensure only suitably qualified and safe individuals work with our learners. Safer recruitment is a preventative control linked to our safeguarding risk assessments and our ISO 9001 competence management approach.

1) Job descriptions (JDs)

- Every JD clearly states safeguarding responsibilities, expected conduct, mandatory training, and reporting lines to the DSL.
- Role-specific technical and HSE competencies (e.g., assessor/invigilator requirements) are listed alongside behavioral expectations (ethics, boundaries, confidentiality).

2) Identity and credential checks

- Original ID verification (government photo ID) is mandatory before offer.
- Education and professional credentials are checked directly with issuing bodies or via verifiable records. For HSE tutors/assessors, current sector competence and recent CPD must be evidenced.
- Employment history is verified for a minimum of the last five years (or since leaving full-time education), with explanations for gaps.
- Where local law or client contracts require, additional vetting may be completed proportionate to role risk.

3) Reference verification

- At least two references are obtained, including the most recent employer. References must address conduct, safeguarding concerns, and suitability to work with adult learners.
- Verbal verification is preferred to confirm authenticity. Any hesitation or safeguarding indicators trigger a risk review with the DSL before appointment.

4) Interview questions on safeguarding

- Interviews include structured questions that explore professional boundaries, responding to disclosures, managing digital communication, equity and inclusion, and handling conflicts of interest.
- Scenario prompts test candidate judgement (e.g., a learner's distress disclosure; pressure to change a result; inappropriate online contact).
- Interviewers record evidence against criteria and flag risks for DSL review.

5) Probation and supervision

- All new starters complete a probation period with a named mentor. Objectives include code of conduct adherence, secure assessment handling, inclusive practice, and record-keeping.
- Early performance reviews (e.g., weeks 4 and 12) check conduct, learner feedback, and any concerns.
- No unsupervised access to assessment materials or vulnerable learners until mandatory inductions (safeguarding, exam security, HSE) are completed.

6) Role-based vetting (where applicable)

- Higher-risk roles (e.g., exam officers, lone-working tutors, off-site trainers) undergo enhanced checks proportionate to risk assessments and client/TVTC requirements.
- Contractors and visiting speakers sign the Code of Conduct, provide ID, and are supervised unless fully cleared.

7) Record-keeping and improvement

- Recruitment packs (ID, credentials, references, interview notes, risk decisions, training certificates) are controlled records.
- Trends from recruitment issues feed into CAPA, staff training plans, and annual safeguarding reviews.
- Any allegation or low-level concern arising during employment triggers an immediate review of suitability and additional controls.

5. Creating a Safe Learning Environment

We design our learning spaces to be welcoming, respectful, and risk-aware. Safety is built into daily routines, not added on. All staff share responsibility for safeguarding, with the Head of Centre accountable overall, the Designated Safeguarding Lead (DSL) coordinating concerns, and the HSE Officer overseeing environmental and occupational safety controls. We follow a plan–do–check–act cycle so that lessons from audits, incidents, and feedback turn into practical improvements.

Access control & visitor management

- Reception controls entry during operating hours; all visitors sign in, show ID, and receive a clearly visible **Visitor Badge** that states the date, host, and permitted areas.
- Unbadged individuals are challenged and escorted to reception. Contractors are inducted before work starts and supervised as needed.
- Learners are reminded not to tailgate others through controlled doors.

Supervision & boundaries

- Adequate staff–learner ratios are maintained; a responsible staff member is always present when learners are on site.
- One-to-one meetings occur in visible areas or rooms with clear panels; doors remain ajar where practicable.
- Staff follow our Code of Conduct on professional boundaries and communication channels.

Classroom setup & housekeeping

- Rooms are set to prevent trip hazards, with clear aisles and safe cable routing. Seating accommodates diverse needs, including front-row options for hearing/vision support.
- Equipment (projectors, power tools for practicals, lifting/rigging models) is checked before use; defects are tagged “out of service” and reported immediately.
- Safety signage, evacuation maps, and nearest first-aid points are posted and kept current.

First aid & medical readiness

- At least one certified first aider is on duty per shift. First-aid kits are stocked, dated, and inspected monthly; an AED is available where indicated by risk assessment.
- Allergies, medical conditions, and emergency contacts—shared voluntarily—are treated as confidential and accessible on a need-to-know basis.

Emergency procedures

- Fire, medical, and security emergencies follow posted procedures and staff scripts. Drills are conducted at least twice yearly, including for evening or weekend cohorts.
- Assembly points are accessible and signposted. Wardens perform sweep checks; roll call uses class registers.
- Any incident triggers a short debrief and, where relevant, corrective actions and retraining.

Inclusive and accessible facilities

- Entrances, circulation routes, and WCs aim to be accessible; temporary barriers are avoided or mitigated.
- Prayer space and privacy considerations are integrated respectfully into room scheduling.
- Reasonable adjustments are available for learning and assessment; requests are handled confidentially and promptly.

Environmental & OSH considerations for practicals

- Practical activities (e.g., basic HSE demonstrations, safe lifting simulations) have written risk assessments covering PPE, equipment guarding, noise, lighting, ventilation, and ergonomics.
- Controls aim to reduce environmental impact: waste is segregated; hazardous consumables (if any) are minimized and stored safely; energy and water use are monitored.
- Tutors brief learners on local hazards before each session; dynamic risk assessments are updated if conditions change.

Reporting & continuous improvement

- Concerns about safety, conduct, or accessibility can be raised to the DSL, HSE Officer, or Centre Manager, or via **support@reddune.org**. Low-level concerns are welcomed early to prevent escalation.
- We track KPIs such as incident rate, first-aid responses, evacuation drill performance, corrective action closure, and learner safety feedback, and we review them at Quality Review Meetings.

6. Digital & Online Safety

Digital safeguarding protects learners and staff when using Red Dune systems, personal devices on our network, and approved third-party platforms. It covers acceptable use, platform selection, recording and photography, remote delivery, and data minimization.

Acceptable use

- Centre devices and networks are for authorized educational and administrative purposes. Access is role-based; passwords must be strong and private.
- Bullying, harassment, discrimination, explicit or violent content, and unauthorized data sharing are prohibited.
- Staff do not use personal messaging accounts to contact learners; official channels and addresses are used (e.g., **info@reddune.org**, **admissions@reddune.org**, **exam@reddune.org**).

Approved platforms & security

- Only Centre-approved platforms are used for virtual classes, assessments, and file exchange. The IT Administrator maintains an approved list and updates security settings by default.
- Screensharing is limited to required materials; waiting rooms and host controls are enabled to prevent unauthorized access.
- Sensitive files are shared via controlled repositories, not public links.

Recording, photography & consent

- Recording of sessions (audio/video) is **off by default**. If recording is necessary (e.g., for quality assurance), learners are told in advance, the purpose and retention period are stated, and an on-screen notification appears.
- Screenshots or photographs of learners are not permitted unless explicitly approved for a defined educational purpose; faces and names are redacted where feasible.
- Examinations and invigilated assessments follow awarding-body/TVTC rules on any permitted recording or identity checks.

Remote delivery safeguards

- Tutors begin remote sessions with a safety briefing: respectful conduct, camera and microphone etiquette, and how to report concerns.
- For under-supervised environments (home, workplace corners), tutors adjust activities to low risk and avoid encouraging any practical task that requires supervision or PPE unless an approved local supervisor is present.
- Breakout rooms are monitored; private chat between staff and a single learner is avoided unless necessary and, if used, is documented.

Data minimisation & privacy protection

- We collect the minimum personal data needed for learning and assessment and retain it only as long as required by regulation or awarding-body rules.
- Personal identifiers are limited in class lists and displayed screens, group emails use CC where appropriate.
- Access to assessment data is restricted to authorised roles; tamper-evident storage and version control are applied to results and scripts.

Responding to digital concerns

- Harmful content, cyberbullying, impersonation, or platform intrusions are reported immediately to the DSL and IT Administrator. Evidence (timestamps, screenshots) is preserved and handled confidentially.
- Where the concern involves a criminal or safeguarding risk, we escalate to relevant authorities and cooperate fully, while supporting affected learners.

Training, audits & improvement

- All staff complete annual refreshers on digital safeguarding, privacy, and exam security.
- Periodic audits test access controls, platform settings, and recording practices; results feed into corrective and preventive actions.
- Learner feedback on the clarity and comfort of online sessions is reviewed termly to improve accessibility and safety.

7. Corrective & Preventive Action (CAPA)

Purpose
To ensure any safeguarding concern—whether raised by a learner, staff member, visitor, or external party—triggers a structured, time-bound improvement cycle so that risks are controlled, causes are eliminated, and recurrence is prevented. The CAPA approach aligns with PDCA thinking and quality/HSE expectations in ISO 9001, 14001, and 45001, alongside TVTC quality requirements.

When CAPA is required

- Confirmed safeguarding incidents or near-misses (e.g., harassment, bullying, unsafe supervision).
- Audit or monitoring findings (internal or external) that indicate gaps in safeguarding.
- Patterns or trends in complaints, exit feedback, or learner surveys.
- Any breach of data privacy or assessment security that could impact learner safety or wellbeing.

Process Steps

1. **Immediate Containment (Day 0–1):** The Designated Safeguarding Lead (DSL) ensures the person at risk is safe; implements short-term controls (e.g., separating parties, additional supervision, pausing an activity).
2. **Notification & Logging (Day 0–2):** Record the issue on the Safeguarding Incident Log and CAPA Tracker. Notify the Head of Centre (HoC) and Quality Lead. Where applicable, inform relevant external bodies per escalation rules.
3. **Root-Cause Analysis (RCA) (Day 2–7):** The DSL and Quality Lead conduct RCA using proportionate tools (e.g., 5 Whys, Fishbone, task walk-throughs, document reviews). Distinguish between immediate, contributing, and systemic causes (policy gaps, training needs, supervision, environment, communication).
4. **Action Plan (Day 7–10):** Define **Corrective** actions (to fix what happened) and **Preventive** actions (to stop it recurring elsewhere). For each action assign an **owner**, **deadline**, and **success criteria**. Identify any competence, facilities, document-control, or contractor-management changes needed.
5. **Implementation & Communication (By deadline):** Owners complete actions and upload evidence (revised forms, training records, briefings, signage, room layouts). The DSL communicates relevant changes to staff/learners on a need-to-know basis.
6. **Effectiveness Check (Within 30 days of closure):** Verify outcomes via spot-checks, interviews, mini-audits, or observations. Confirm that risks are reduced and behaviours have changed. If not effective, reopen CAPA with escalated controls.
7. **Quality Review Meeting (QRM) Integration:** Summaries of safeguarding CAPAs, trends, and lessons learned are tabled at the termly QRM and in the Annual Management Review for cross-centre learning and resource decisions.

8. Confidentiality & Data Protection

To protect the dignity, privacy, and safety of individuals involved in safeguarding cases by ensuring information is collected, used, stored, and shared lawfully, fairly, and only on a need-to-know basis. This safeguards trust while enabling timely protection actions and compliance with TVTC expectations and ISO management system controls.

Principles

- **Need-to-Know Sharing:** Share the minimum information with the fewest appropriate people to keep someone safe or to meet regulatory obligations.
- **Lawful, Fair, Transparent:** Explain to the data subject (where safe and appropriate) what we will do with their information and why.
- **Accuracy & Timeliness:** Keep records factual, dated, and updated promptly.
- **Security by Design:** Apply physical, technical, and procedural controls throughout the case lifecycle.
- **Retention & Disposal:** Keep data no longer than necessary; dispose securely.

Roles

- **DSL (Information Custodian):** Controls access to safeguarding case files, approves sharing decisions, and holds the master register.
- **Head of Centre:** Final authority for high-risk sharing decisions and external disclosures when required.
- **Admin/Records Officer:** Maintains secure filing, applies retention rules, manages redaction requests under instruction.
- **All Staff:** Use only approved channels; never store safeguarding data on personal devices.

Collection & Recording

- Use the Safeguarding Concern Form and Case File templates. Record objective facts (what, when, who), observed impact, immediate controls, and decisions taken. Avoid opinion unless clearly labelled as professional judgment.
- Attach relevant evidence (emails, screenshots, CCTV references) following chain-of-custody practices where applicable.

Storage & Access Controls

- **Digital:** Encrypted drive/folder with role-based permissions; multi-factor authentication; audit trail enabled.
- **Paper:** Numbered files, tamper-evident cabinet in a restricted office; sign-in/out log.
- **Email:** Use **complaints@reddune.org** (for reporting) and DSL mailbox for case handling; avoid unprotected forwarding. Redact identifiers where full detail is unnecessary.

Sharing & Redaction

- Internally, share only with those directly involved in safeguarding action (DSL team, HoC, relevant manager, assessor if needed for adjustments).
- Externally, disclose to awarding bodies, TVTC, or competent authorities where mandated or necessary to protect individuals. Record the legal/operational basis for sharing.
- Redact names, IDs, and sensitive details when broader communication is required (e.g., general safety alerts, QRM packs).

Retention & Disposal

- Follow the Records Retention Schedule: safeguarding case files kept for the defined period appropriate to risk/age and regulatory needs, then securely destroyed (cross-cut shredding or certified digital wipe). Log all disposals.

Data Breach Response

- Suspected breaches (mis-sent email, lost device, unauthorized access) must be reported immediately to the DSL and Head of Centre. Contain, assess impact, notify affected parties and authorities where required, and raise a CAPA entry. Brief involved staff to prevent recurrence.

Training & Awareness

- Mandatory induction for all roles; annual refresher covering confidentiality limits, safe communications, and secure handling. Targeted training for DSL/admin on redaction and evidence handling.

Assurance & Continual Improvement

- Periodic internal audits test access controls, retention accuracy, and sharing decisions. Results feed CAPA and the QRM. Lessons learned update forms, scripts, and staff guidance.