REDDUNE TRAINING CETNER

INVESTIGATION POLICY

THIS PROCEDURE IS CONTROLLED BY RED DUNE TRAINING 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	10 Jun, 2022	14 Jun, 2022

REVISION HISTORY

REVISION	DATE	REMARKS
1	10 Aug, 2024	
2	16 Aug, 2025	

RED DUNE

Investigation Policy

Contents

1. Policy statement & objectives 3
2. Scope 4
3. Definitions 5
4. Triggers & intake channels 6
5. Initial triage & risk rating 7
6. Case registration & confidentiality 8
7. Evidence preservation & chain of custody 9
8. Notification & escalation rules 11
9. Investigative plan 12

1. Policy statement & objectives

Red Dune Training Centre (Saudi Arabia) is committed to conducting fair, timely, and evidence-based investigations into any alleged malpractice, maladministration, assessment irregularity, unsafe act/condition, environmental incident, data/privacy breach, or unethical conduct connected to our training, assessment, and Centre operations. We operate a zero-tolerance approach to intentional wrongdoing and require all staff, contractors, learners, and partners to cooperate fully with investigations. All cases will be handled impartially, with confidentiality, dignity, and without victimization or retaliation toward any party who raises a concern in good faith. Where risks to health, safety, environment, or assessment integrity are identified, we will take immediate controls, followed by root-cause analysis and corrective and preventive actions. Outcomes from investigations feed directly into our quality, HSE, and environmental management reviews to drive continual improvement.

Objectives

1. **Integrity & Fairness:** Ensure each case is assessed on facts, using consistent procedures, independent decision-making, and the balance-of-probabilities standard.
2. **Timeliness:** Acknowledge concerns promptly, triage risk quickly, and conclude investigations within defined service levels, escalating where necessary.
3. **Evidence Management:** Secure, preserve, and document all relevant evidence (e.g., scripts, logs, digital records, CCTV, witness statements) with clear chain-of-custody.
4. **Learner Protection:** Safeguard learners' rights, reasonable adjustments, and access to learning while investigations are ongoing, unless safety or integrity would be compromised.
5. **Health, Safety & Environment:** Prioritise immediate hazard control and legal/regulatory notifications for incidents impacting people or the environment.
6. **Transparency & Confidentiality:** Communicate clearly, share outcomes on a need-to-know basis, protect personal data, and record decisions with documented rationales.
7. **Compliance:** Align investigation practice with applicable Saudi requirements and awarding/recognition body expectations for assessment security and centre conduct.
8. **Improvement:** Translate findings into corrective and preventive actions, update risk registers and procedures, brief staff, and verify effectiveness through audits and reviews.
9. **Competence:** Ensure investigators and relevant staff are trained, current, and periodically calibrated to maintain consistent quality across cases.

2. Scope

This Investigation Policy applies to all activities of Red Dune Training Centre (Saudi Arabia) that may give rise to concerns, incidents, or allegations requiring a formal, evidence-based inquiry. It covers all staff (permanent, temporary, and agency), tutors/assessors/invigilators, IQA/quality personnel, contractors, consultants, suppliers, visitors, and all learners/candidates enrolled on international qualifications or TVTC-approved programmes, across all delivery modes (in-person, blended, online, on-site at client premises) and all locations under our operational control.

Assessment irregularities and exam security — Suspected cheating, plagiarism, collusion, identity fraud, breach of invigilation rules, misuse of materials/devices, tampering with results, unauthorized access to assessments, or failure to follow approved assessment conditions.

Malpractice and maladministration — Any deliberate or negligent act that compromises integrity or compliance, including falsification of records, misuse of Centre approvals, conflicts of interest not declared/managed, and procedural failures affecting learners, staff, awarding bodies, or TVTC.

HSE / OH&S incidents — Work-related injuries, illnesses, near misses, unsafe acts/conditions, emergency responses during teaching/assessing/practical work, including contractor and visitor activities that interact with our operations.

Environmental incidents — Actual or potential pollution, spills, waste mismanagement, excessive resource use, or nonconformities with environmental controls linked to training or assessment activities.

Safeguarding — Concerns about learner welfare, abuse, harassment, bullying, discrimination, or exploitation within centre influence, including online environments.

Data/privacy breaches — Personal data loss, unauthorized disclosure, system intrusion, or misuse of assessment/sensitive information.

Complaints and whistleblowing — Allegations or disclosures from any stakeholder (internal or external) about wrongdoing, risks, or non-compliance; protected disclosures are covered, and whistleblowers are safeguarded against retaliation.

This scope extends to incidents arising from third-party provision (e.g., proctoring, content hosting, venue hire) where they affect our learners, assessments, or compliance obligations. Interfaces with other procedures (Appeals, Complaints, Safeguarding, HSE, Environmental, Data Protection, Disciplinary, and CAPA) are managed to ensure a single, coordinated investigation path, consistent with TVTC requirements and the expectations of international awarding bodies and ISO 9001/14001/45001.

3. Definitions

Malpractice — Any deliberate or reckless act or omission that compromises integrity, fairness, or safety of teaching, assessment, certification, or records. Examples include cheating, collusion, falsifying results, impersonation, bribery, or knowingly breaching exam security.

Maladministration — Unintentional or systemic poor administration that leads to error, inconsistency, or non-compliance. Examples: using obsolete forms, mishandling scripts, weak ID checks, or failing to apply approved procedures and timelines.

Conflict of Interest (COI) — Any situation where personal, financial, or professional interests could improperly influence a person's judgement or give the appearance of bias (e.g., assessing a relative, commercial gain, prior close supervision). Declared COIs must be managed or removed before involvement.

Irregularity — Any departure from approved assessment or administrative procedures, whether intent is proven. Includes timing deviations, room breaches, missing records, or use of unauthorized materials or equipment.

Incident — An unplanned event that affects or could affect academic integrity, learner welfare, health and safety, environment, data privacy, or property. Includes security breaches, injuries, spills, fire alarms, or IT outages during assessment.

Near Miss — An unplanned event that did not result in harm or loss this time, but had the potential to do so (e.g., unlocked exam cabinet found, proctoring camera offline, trailing cable in exam room). Near misses are recorded and investigated to prevent recurrence.

Whistleblower — A person who, in good faith, raises a concern about wrongdoing, risk, or non-compliance that they reasonably believe is in the public interest or necessary to protect learners, staff, or the awarding process. Protection applies regardless of role or contract.

Protected Disclosure — A report made in good faith through approved channels, containing information the reporter reasonably believes shows malpractice, maladministration, or risk to health, safety, environment, or legality. Retaliation for such disclosures is prohibited.

Complainant — The individual or organization submitting a complaint or appeal about a decision, behavior, process, or outcome related to training or assessment. May be a learner, client, staff member, contractor, or visitor.

Respondent — The person or unit alleged to have engaged in the behavior or process under review, or whose decision is being challenged. The respondent is entitled to be informed of the case, respond, and be treated fairly and without prejudice.

Interpretation notes: Terms apply across TVTC-regulated and international programmes; definitions guide triage, evidence collection, sanctions, and corrective actions and improvements.

4. Triggers & intake channels

To define what initiates an investigation at Red Dune Training Centre (Saudi Arabia) and how concerns are received, recorded, and triaged in line with international bodies and TVTC expectations and ISO 9001/14001/45001 good practice.

What starts an investigation (Triggers)
An investigation may be opened when any of the following are reported or detected:

- **Assessment irregularities:** invigilation breaches, impersonation, plagiarism/AI misuse, collusion, unauthorized materials, or script tampering.
- **Malpractice/maladministration:** falsified records, conflict of interest, misuse of certificates, or non-adherence to approved procedures.
- **Learner or staff concerns:** allegations of unfair marking, discrimination, bullying/harassment, safeguarding issues, or fitness-to-assess concerns.
- **HSE/OH&S/Environmental events:** incidents or near misses during training/assessment, unsafe conditions, equipment failure, chemical or waste spills, breaches of environmental controls.
- **Information security/privacy:** suspected data breach, loss of assessment materials, unauthorized disclosure of personal data.
- **Audit and oversight signals:** findings from internal audits, IQA sampling, external verifier reports, awarding-body or TVTC notifications, or trend anomalies in KPIs.
- **External intelligence:** credible client/employer complaints, partner alerts, or substantiated social-media reports relevant to Centre operations.

How concerns are received (Intake Channels)

- **Email:** complaints@reddune.org (general/whistleblowing), exam@reddune.org (assessment/security), support@reddune.org (learner services).
- **Online form/website:** submissions via reddune.org contact page or designated incident/appeal forms.
- **In person:** to the Office Coordinator, Invigilator, Assessor, Quality Lead/IQA, Centre Manager, or Head of Centre.
- **Physical forms:** incident, concern, or invigilation reports available at reception/exam rooms.

Assurances & Handling

- Reports may be **anonymous**; confidentiality and non-retaliation are upheld.
- All submissions receive a **case ID** and are logged in the secure Incident/Concern Register.
- **Immediate escalation** occurs where there is imminent risk to health, safety, environment, exam security, or data protection.
- Acknowledgement is issued within **24 working Hors**; **triage within 48 working Hours** to determine scope, risk rating, and next steps.
- Evidence (scripts, logs, CCTV, photos, emails) is preserved under chain-of-custody controls and handled on a “need-to-know” basis.

5. Initial triage & risk rating

Purpose
To sort every reported concern quickly and consistently, protecting learners, staff, the environment, and assessment integrity while meeting TVTC and international awarding-body expectations and ISO 9001/14001/45001 risk-based requirements.

Triage steps (within 24 working Hours, sooner if safety-critical)

1. **Stabilise & preserve:** Make the situation safe; secure evidence (scripts, logs, CCTV, emails, devices).
2. **Register:** Assign a unique case ID and log reporter, summary, date/time, and immediate controls applied.
3. **Screen for conflicts & sensitivity:** Allocate an Investigation Lead with no conflict of interest; mark cases involving minors, health data, or exam security as "restricted."

Severity–Likelihood Matrix (5×5)
Rate each dimension across five impact domains: **Safety (OH&S)**, **Environmental**, **Academic Integrity/Exam Security**, **Reputational**, **Legal/Compliance**.

- **Severity (S):** 1 Trivial → 5 Catastrophic (e.g., life-altering injury; significant release; mass exam compromise; regulatory breach).
- **Likelihood (L):** 1 Rare → 5 Almost certain (based on evidence and controls).
- **Risk score:** R = S × L (1–25).
- **Bands:** 1–5 Low, 6–10 Moderate, 11–15 High, 16–25 Critical.

Decision Tree: Fast-Track vs Full Investigation

- **Critical (16–25):** Immediate controls; notify Head of Centre; consider notifying awarding body/TVTC/regulator; appoint panel; **Full Investigation** mandatory with root-cause analysis and CAPA; target start ≤24 hours.
- **High (11–15):** Escalate to HoC; determine external notification need; **Full Investigation** unless clearly contained; start ≤3 working days.
- **Moderate (6–10): Fast-Track Review** by Investigation Lead (document review + 1–2 interviews); convert to Full if new facts increase risk; close ≤10 working days.
- **Low (1–5): Fast-Track Resolution** (coaching, minor correction, local CAPA), with evidence preserved and management sign-off.

Consistency & Documentation
Record the matrix scoring for each domain, rationale, interim controls, and chosen pathway. Update risk if new evidence arises. Bias checks (second reviewer) apply to exam security and safeguarding cases.

Outputs
A triage note, risk heat-map snapshot, notification log, and an initial CAPA plan (owner, due date, verification method) filed under the case ID.

6. Case registration & confidentiality

Every investigation opened by Red Dune Training Centre (Saudi Arabia) is registered immediately in the secure **Case Log** and assigned a **Unique Case ID** (format: RD-INV-YYYY-####). The Case ID is used on all documents, emails, interview notes, evidence labels, corrective-action records, and reports to avoid using personal identifiers in open text and to protect privacy.

Secure log & access control.
The Case Log is a controlled record held within our quality system. Access is strictly **role-based** (Head of Centre, Investigation Lead, Quality Lead/IQA, and, where relevant, HSE Officer or Data Protection Lead). Permissions are granted on the principle of **least privilege** and reviewed at each stage of the case. Electronic files are stored in a restricted workspace with audit trails; hard copies are sealed, signed across the seal, and stored in a locked cabinet. Chain-of-custody entries capture who collected, created, viewed, or transferred each item, with date/time stamps.

Confidentiality undertakings.
All participants (investigators, interviewers, note-takers, witnesses, subject specialists) sign a short **Confidentiality & Conflict-of-Interest Statement** before receiving case information. Interviews are conducted in private, with need-to-know disclosure only. Case materials are not removed from controlled locations or shared via personal devices.

Anti-retaliation protections.
No learner, employee, contractor, or visitor will be disadvantaged, threatened, or harassed for raising a concern or cooperating with an investigation. Allegations of retaliation are treated as separate potential misconduct and investigated with priority. Where risk is identified, the Centre may apply temporary safeguards (e.g., timetable adjustments, alternative invigilation, separation of parties).

Data handling & retention.
Personal data are minimized and redacted where possible. Case files are retained and disposed of per our Records Retention Schedule and applicable awarding-body/TVTC requirements. Any external sharing (e.g., with awarding bodies or regulators) uses secure channels, with redaction as required.

Assurance.
Compliance with these controls is checked during internal audits and management review. Breaches of confidentiality or access rules trigger immediate corrective action and may lead to disciplinary measures.

7. Evidence preservation & chain of custody

To protect the integrity, authenticity, and admissibility of evidence gathered during investigations at Red Dune Training Centre (Saudi Arabia). This section ensures secure preservation, transparent traceability, and controlled access from first discovery to final archival or lawful disposal, consistent with recognized awarding-body expectations and ISO management-system practice.

Scope
Applies to all investigation evidence, including assessment materials (question papers, scripts, mark sheets), exam-room artefacts (CCTV, seating plans, invigilation logs), digital learning records (LMS data, login trails), correspondence (emails, messages), photographs/videos, equipment checklists, HSE/environmental incident records, and any physical items relevant to the case.

Collection Principles

1. **Prompt, safe, systematic:** Stabilise the scene, stop further loss or contamination, and record conditions.
2. **Least-intrusive capture:** Prefer forensic images/copies over originals where feasible; document any unavoidable handling of originals.
3. **Context preserved:** Photograph overall view, mid-range, and close-ups; note dates, times, locations, and identifiers visible in images.

Secure Storage

- **Physical:** locked fire-resistant cabinet/room with restricted key control and access logs; temperature and humidity considered for sensitive media.
- **Digital:** encrypted vaults or secure drives with role-based permissions, multi-factor authentication, write-blocked intake, and regular integrity checks. Originals are set to read-only; analysis occurs on verified copies.

Digital Forensics & Integrity
For electronic evidence (LMS exports, emails, device images, CCTV files), the EO/IT Admin generates cryptographic hashes (e.g., SHA-256) at acquisition and after transfers to confirm immutability. Forensic images are created using approved tools; working copies are clearly distinguished and documented.

Special Items

- **CCTV:** export the relevant timeframe with player/codec details and verify playback; preserve the full original segment when viable.
- **Assessment Scripts:** include seating plans, invigilation logs, attendance registers, and any special-consideration forms to maintain context.
- **Hazardous/biological materials:** if ever applicable (e.g., contaminated PPE from an incident), store separately and safely, with additional controls per HSE guidance.

Access & Review Controls
Access is “need-to-know” and time-bound. Viewing sessions are pre-booked, supervised, and recorded in the log. Copies for external reviewers are minimized and tracked; redactions are documented and approved by the IL.

Retention & Disposal
Retention periods follow applicable awarding-body/TVTC requirements and our Records Retention

Schedule. On expiry, disposal is secure and evidenced: cross-cut shredding for paper, certified destruction for media, and cryptographic wipe for digital storage. Disposal entries include method, date, and witnesses.

Assurance & Improvement
Periodic internal audits, spot seal checks, and reconciliation of registers verify ongoing control. Any nonconformity triggers corrective action, with lessons learned feeding into staff training, assessment security measures, and system updates. Continuous improvement actions are reviewed at the Quality Review Meeting.

8. Notification & escalation rules

Ensure timely, accurate notification to internal leaders, TVTC, international awarding bodies insurers, and authorities where required, consistent with ISO 9001/14001/45001 and Saudi legal expectations.

When to notify (triggers)

1. **Assessment integrity:** suspected malpractice/maladministration, exam security breaches, systemic marking errors, data anomalies impacting results.
2. **OH&S incidents:** work-related injury, dangerous occurrence, fire, or near-miss of significant potential.
3. **Environmental incidents:** spills, emissions, or waste non-conformities linked to training/assessment activity.
4. **Data/privacy events:** loss, unauthorised access, or disclosure of assessment or personal data.
5. **Safeguarding/ethical concerns:** credible allegations affecting learner safety or fairness.
6. **Material operational disruption:** events that may compromise scheduled assessments or certification.

Timeframes (from awareness)

- **Internal:** HoC and Quality Lead within **20 hours**; initial incident log within **24 working Hours**.
- **Awarding body/TVTC:** "at once" for serious exam security or safety events; otherwise, an initial notification within **24 working Hours**, with a full report within **48–72 working hours** or per the body's stated SLA.
- **Insurer/broker:** within **24 hours** for events with potential liability.
- **Authorities/regulators:** as required by Saudi law for OH&S/environmental events (HSE Officer to confirm statutory windows).

How to notify (formats & channels)

- Use the awarding body/TVTC prescribed forms/portals where available; attach the **Incident/Investigation Intake Form**, chain-of-custody log, witness statements, and evidence index.
- Email submissions should be authorized by the HoC and sent from official accounts (e.g., **complaints@reddune.org**, **exam@reddune.org**), with the case ID in the subject line.
- For urgent risks, phone the relevant contact first, then follow with written confirmation.
- Provide clear, factual summaries; avoid speculative language; mark documents "Confidential—Investigation Material."

Escalation path
Investigation Lead → Quality Lead/IQA → HoC (approval) → External body/TVTC/insurer. If conflicts of interest exist, appoint an alternate signatory.

Recordkeeping & follow-up
Capture all notifications, acknowledgements, and deadlines in the Investigation Register. Track required actions from TVTC/awarding bodies/insurers and report status at the next Quality Review Meeting. Outcomes feed into CAPA and management review to support continual improvement.

9. Investigative plan

This section sets out how Red Dune Training Centre will plan each investigation, so it is fair, timely, proportionate, and defensible. The plan translates an allegation or incident into clear tasks, responsibilities, and evidence needs, while respecting learner rights, exam security, and health, safety, and environmental considerations.

1) Scope
Define the exact boundaries of the case before any interviews start. Specify: the programmes/assessment or activity involved; the locations (classroom, online platform, off-site); the date range; the individuals and suppliers in scope; and what is explicitly out of scope. Record assumptions and constraints (e.g., limited CCTV coverage, external venue rules). Note any related cases to avoid overlap or conflict.

2) Issues and Lines of Enquiry
List the precise questions the investigation must answer (e.g., "Were assessment conditions breached?", "Did any act create HSE risk?", "Was there maladministration?"). For each question, note the evidence type required to prove or refute it and the decision standard ("balance of probabilities"). Include compliance checks against internal procedures and awarding/TVTC requirements.

3) Witness Map
Create a witness matrix naming complainant(s), respondent(s), invigilators, assessors, learners, administrators, and any third parties (venue staff, contractors). Priorities critical witnesses, identify potential conflicts of interest, and assign an interviewer and note-taker for each interview. Capture availability, preferred language, and whether support persons are requested.

4) Documents & Evidence
Produce an evidence checklist and collection plan covering assessment papers/marking guides, scripts, attendance sheets, seating plans, invigilation logs, version-controlled documents, e-mails, LMS/assessment platform logs, access control records, calibration/maintenance records for equipment used, incident/near-miss reports, CCTV or photographs. Establish chain of custody with unique case IDs, timestamps, storage location, and permissions. Mark sensitive personal data and restrict access on a need-to-know basis. Note any environmental or OH&S monitoring data relevant to the incident.

5) Schedule & Milestones
Lay out a dated timeline with service levels: acknowledgement, triage, evidence preservation, interviews, analysis, draft findings, quality review, decision issue, and CAPA (corrective and preventive actions) assignment. Include dependencies (e.g., external examiner availability, venue approvals). Add buffers for translation, public holidays, or travel to remote sites. Confirm how urgent risks will be controlled while the investigation proceeds.

6) Language & Translation
Record the working language of the investigation and any translation needs for interviews, statements, forms, or technical evidence. Appoint competent translators/interpreters who are briefed on confidentiality and neutrality. When documents exist in multiple languages, identify the authoritative version for decision-making and ensure back-translation for accuracy where outcomes are high-stakes.

7) Accessibility & Adjustments
Identify any reasonable adjustments for participants: accessible rooms, prayer breaks, gender-appropriate interviewers where culturally appropriate, virtual interviews for those off-site, extended

time for those with documented needs, or assistive technology. Record the rationale for each adjustment so fairness and consistency are demonstrable.

8) Risk, HSE and Environmental Controls
Assess immediate risks associated with the case (e.g., exam integrity, safety hazards, environmental harm, data security). Define interim controls—such as supervised re-assessment conditions, temporary removal of an assessment instrument, or isolating equipment/areas pending inspection. Ensure the plan does not compromise safety or environmental controls during evidence collection.

9) Roles, Approvals & Communications
Name the Investigation Lead, reviewer/quality checker, and decision maker (separate from the investigator). Set the approval path for the plan and the format for updates (status report frequency, distribution list, confidentiality markers). Pre-draft stakeholder messages for key milestones to avoid delays and ensure consistent, neutral language.

10) Review & Closeout Criteria
Define what "complete" looks like: all lines of enquiry answered, evidence indexed, interviews signed, analysis documented, findings reviewed for bias/conflict, and CAPA raised with owners and deadlines. State the retention category for the case file and how lessons learned will flow to training, assessment design, invigilation, HSE procedures, and staff CPD.

This structured plan ensures each case is handled consistently, with clear scope, documented decisions, protected evidence, and appropriate respect for participants' rights and safety.