Universal Acceptable Use Requirements for TCT Platforms, Services and Learning Resources

Document status: External policy
Policy owner: Transact Connect Training (Pty) Ltd
Version: 1.1
Effective date: 20 January 2025
Last reviewed: 28 July 2026
Next scheduled review: Within 12 months of the effective date
Website: www.transacttraining.online
Contact: legal@transacttraining.online

---

1. Purpose

1.1 This Acceptable Use Policy establishes the rules governing access to and use of the platforms, systems, Courses, Course Materials and related services provided by Transact Connect Training (Pty) Ltd.

1.2 The purposes of this Policy are to:

- Protect learners and other authorised users;
- Protect TCT's systems, Course Materials and intellectual property;
- Protect Client Organisation and learner information;
- Maintain the integrity of learning and assessment activities;
- Prevent unlawful, harmful, abusive or unauthorised conduct;
- Establish clear security and account-use requirements;
- Support reliable and professional delivery of TCT Services;
- Define the consequences of misuse; and
- Provide a consistent standard across all current and future TCT clients and users.

1.3 This Policy applies whether access is:

- Purchased by an individual;
- Sponsored by an employer;
- Provided through a Client Organisation;
- Provided through a TCT Academy;
- Granted for administration, facilitation or assessment;
- Provided on a trial, demonstration or complimentary basis; or
- Otherwise 1uthorized by TCT.

2. Scope

2.1This Policy applies to:

- Learners;
- Prospective learners;
- Individual purchasers;
- Client Organisations;
- Sponsors;
- Client administrators;
- Academy administrators;
- Facilitators;
- Assessors;
- Consultants;
- Contractors;
- Suppliers;
- Implementation partners;
- Authorised guests;
- TCT employees; and
- Any other person who accesses or uses TCT Services.

2.2 This Policy applies to the use of:

- The TCT learning management system;
- TCT websites and portals;
- TCT Courses, modules, units and learning pathways;
- Course Materials;
- Assessments and assignments;
- Digital Certificates;
- AI-enabled learning tools;
- Role-plays and simulations;
- Virtual classroom and facilitated sessions;
- Discussion, messaging and collaboration functions;
- Downloads and templates;
- Administrative dashboards;
- Learner reports;
- Application programming interfaces and integrations;
- Support systems;
- Email and other communications connected to TCT Services;
- TCT-provided user credentials;
- TCT-branded Academies; and
- Any other system, platform or resource made available by or on behalf of TCT.

© Business Confidential

2.3 This Policy applies regardless of:

- The User's location;
- The device used;
- Whether access occurs through a personal or business network;
- Whether the Services are hosted by TCT or a third party;
- Whether the User is actively studying or performing an administrative function; or
- Whether the activity occurs during or outside normal business hours.

3. Relationship with other TCT documents

3.1 This Policy forms part of the rules governing use of TCT Services and must be read together with:

- The TCT Terms of Service;
- The TCT Privacy and Data Protection Policy;
- The TCT AI Acceptable Use Policy;
- The TCT Academic Integrity Policy;
- The TCT Information Security Policy;
- The TCT Anti-Bribery and Anti-Corruption Policy;
- The TCT Complaints and Appeals Policy;
- Any applicable Client Agreement;
- Any Course-specific requirements; and
- Any lawful instruction communicated by TCT.

3.2 Acceptance of the TCT Terms of Service includes an undertaking to comply with this Policy.

3.3 A Client Organisation must take reasonable steps to ensure that its learners, administrators and other authorised users are informed of and comply with this Policy.

3.4 Where a more specific TCT policy governs particular conduct, that policy must be applied together with this Policy.

3.5 A Client Agreement may impose additional requirements but may not authorise conduct that is unlawful, compromises security, infringes intellectual property or undermines learning integrity.

4. Legal and regulatory framework

4.1 Users must comply with all laws and regulations applicable to their access to and use of the Services.

© Business Confidential

4.2 Relevant South African legislation includes:

- The Electronic Communications and Transactions Act 25 of 2002, which regulates electronic communications and transactions and addresses the prevention of abuse of information systems;
- The Cybercrimes Act 19 of 2020, which creates offences relating to unlawful access, interception, interference and other cybercrime-related conduct;
- The Protection of Personal Information Act 4 of 2013, which establishes requirements for lawful and secure processing of personal information; and
- The Copyright Act 98 of 1978, which regulates copyright and the protection of protected works.

4.3 Users outside South Africa must also comply with laws applicable in their own jurisdictions.

4.4 Nothing in this Policy authorises activity that would otherwise be unlawful.

5. Definitions

For purposes of this Policy:

5.1 “Account”
Means the personal, learner, facilitator or administrative profile through which a User accesses the Services.

5.2 “Administrator”
Means a person authorised by TCT or a Client Organisation to manage learners, enrolments, reporting or other Platform functions.

5.3 “AI Tools”
Means artificial intelligence, automated role-play, simulation, chatbot, knowledge-exploration, content-generation or similar functionality made available by or through TCT.

5.4 “Client Agreement”
Means any master services agreement, academy agreement, proposal, order, schedule, statement of work or other agreement between TCT and a Client Organisation.

5.5 “Client Organisation”
Means an employer, bank, fintech, financial institution, business, public body, educational institution, sponsor, partner or other organisation that purchases, sponsors, administers or facilitates access to TCT Services.

5.6 “Course Materials”
Means all text, videos, audio, illustrations, graphics, presentations, assessments, scenarios, role-plays, simulations, templates, questions, answers, downloads, recordings, frameworks, data and other learning content made available by TCT.

© Business Confidential

5.7 “Credentials”
Means usernames, passwords, authentication codes, tokens, access links and other information used to access an Account or system.

5.8 “Malicious Code”
Means software, scripts, files or instructions intended or reasonably likely to damage, disrupt, compromise, intercept or gain unauthorised access to a system or information.

5.9 “Platform”
Means the TCT LMS, website, portal, application or related digital environment.

5.10 “Services”
Means the Platform, Courses, Course Materials, assessments, Certificates, AI Tools, facilitated sessions, support, reporting and related services provided by TCT.

5.11 “User”
Means any person who accesses or uses the Services.

5.12 “User Content”
Means information, files, responses, prompts, messages, recordings, submissions, comments or other content submitted by a User through the Services.

6. General acceptable-use standard

6.1 Users must use the Services:

- Lawfully;
- Honestly;
- Professionally;
- Responsibly;
- Securely;
- Respectfully;
- For an authorised purpose;
- Within the scope of the access granted; and
- In accordance with this Policy and all other applicable requirements.

6.2 Users must exercise reasonable care to avoid:

- Harming TCT;
- Harming another User;
- Compromising a Client Organisation;
- Disclosing confidential information;
- Disrupting the Platform;
- Undermining assessment integrity;
- Infringing intellectual-property rights;
- Creating security risks; or
- Damaging the reputation or legitimate interests of another party.

6.3 Users must follow reasonable instructions issued by:

- TCT;
- An authorised facilitator;
- An authorised assessor;
- A Platform administrator;
- A support representative; or
- An authorised Client Organisation representative.

6.4 A User who is uncertain whether a proposed activity is permitted must obtain written clarification before proceeding.

7. Authorised purposes

The Services may be used only for legitimate purposes including:

7.1 Personal professional learning and development.

7.2 Employer-sponsored learning.

7.3 Participation in an authorised TCT Course or Academy.

7.4 Completion of permitted assessments and learning activities.

7.5 Participation in facilitated sessions, simulations and role-plays.

7.6 Authorised learner administration and reporting.

7.7 Provision of authorised facilitation, assessment or support.

7.8 Evaluation of TCT Services by a prospective client where TCT has provided demonstration or trial access.

7.9 Use expressly authorised under a Client Agreement.

7.10 Other purposes approved in writing by TCT.

8. Account ownership and personal use

8.1 Each Account is personal to the individual to whom it is assigned.

8.2 A User may not:

- Share Credentials;
- Permit another person to use the Account;
- Use another person's Account;
- Log in on behalf of another learner;
- Complete activities for another learner;
- Rotate an Account among multiple people;

© Business Confidential

- Transfer an Account without approval;
- Sell or lend access;
- Allow concurrent use by multiple persons;
- Create duplicate Accounts to obtain additional access;
- Use a false identity; or
- Misrepresent the person using the Account.

8.3 A User must immediately notify TCT if the User suspects that Credentials have been:

- Disclosed;
- Stolen;
- Guessed;
- Compromised;
- Used by another person; or
- Otherwise placed at risk.

8.4 A User must not use Credentials received in error.

8.5 An Account may be accessed from more than one legitimate device by its assigned User, provided that:

- The devices are secure;
- The Account is not shared;
- The access does not circumvent capacity or licensing restrictions; and
- The use is consistent with the applicable Client Agreement.

9. Password and authentication requirements

9.1 Users must:

- Use passwords that are reasonably strong;
- Keep passwords confidential;
- Avoid reusing a TCT password on unrelated services where reasonably possible;
- Protect authentication codes;
- Complete multi-factor authentication where enabled;
- Lock devices when unattended;
- Log out of shared or public devices; and
- Follow any password-reset instruction issued by TCT.

9.2 Users must not:

- Write passwords where they are openly visible;
- Send passwords through unsecured communications;
- Store passwords in an unprotected document;
- Ask another person for that person's password;
- Attempt to obtain another User's Credentials; or
- Approve an authentication request that the User did not initiate.

© Business Confidential

9.3 TCT may require:

- A password reset;
- Additional verification;
- Multi-factor authentication;
- Reconfirmation of identity; or
- Temporary suspension,

where it reasonably suspects that an Account has been compromised.

10. Device and network responsibilities

10.1 Users are responsible for taking reasonable steps to protect devices used to access the Services.

10.2 Users should, where reasonably practicable:

- Keep operating systems and applications updated;
- Use supported browsers;
- Use anti-malware protection;
- Enable device locking;
- Protect devices against unauthorised physical access;
- Avoid insecure public devices;
- Avoid untrusted networks;
- Back up authorised work appropriately; and
- Follow the security requirements of their Client Organisation.

10.3 A User must not knowingly access the Services from:

- A compromised device;
- A device containing malicious code;
- A device configured to intercept another person's information; or
- A network being used for unlawful activity.

10.4 TCT may restrict access from:

- Unsupported devices;
- Unusual locations;
- Anonymising infrastructure;
- Compromised networks;
- High-risk technical environments; or
- Devices presenting a material security risk.

11. Security-related prohibited conduct

A User must not, without TCT's prior written authorisation:

11.1 Access or attempt to access an Account, system, file, report, Course or area for which the User has not been authorised.

11.2 Probe, scan or test a Platform vulnerability.

11.3 Perform penetration testing, vulnerability testing, load testing or security research.

11.4 Attempt to bypass or defeat:

- Authentication;
- Access controls;
- Course sequencing;
- Assessment restrictions;
- Learner limits;
- Seat limits;
- Access-expiry controls;
- Download controls;
- Monitoring;
- Logging;
- Rate limits;
- Certificate requirements; or
- Other technical safeguards.

11.5 Intercept, monitor or record Platform communications or data without authority.

11.6 Introduce or transmit:

- Malware;
- Viruses;
- Ransomware;
- Spyware;
- Keyloggers;
- Harmful scripts;
- Corrupted files;
- Automated attack tools; or
- Other Malicious Code.

11.7 Disrupt or attempt to disrupt:

- Platform availability;
- Network performance;
- User sessions;
- Assessments;
- Data integrity;
- Support systems; or
- Third-party services used by TCT.

11.8 Conduct a denial-of-service or resource-exhaustion activity.

11.9 Modify, delete, corrupt or interfere with information without authority.

11.10 Disable or interfere with:

- Logging;
- Monitoring;
- Security controls;
- Audit trails;
- Malware protection; or
- Incident-response functions.

11.11 Use another person's authentication session, token or access link.

11.12 Exploit a technical error to obtain access, benefits, results or information not intended for the User.

11.13 Continue using an identified vulnerability after becoming aware that the activity is unauthorised.

11.14 Publish or disclose a suspected vulnerability before TCT has been notified and given a reasonable opportunity to investigate and address it.

12. Automated access and extraction

12.1 Users may not use bots, scripts, crawlers, scraping tools, browser automation or similar methods to access the Services unless TCT has authorised the use in writing.

12.2 Prohibited automated activity includes:

- Scraping Course Materials;
- Bulk downloading;
- Copying assessment questions;
- Extracting learner information;
- Harvesting email addresses;
- Indexing restricted content;
- Replicating Platform functionality;
- Automating Course completion;
- Automating assessment submissions;
- Creating artificial Platform activity; and
- Circumventing reasonable usage limits.

© Business Confidential

12.3 Approved integrations must operate only:

- Within documented permissions;
- For the agreed purpose;
- Using approved Credentials;
- In accordance with rate limits;
- With appropriate security; and
- Under the applicable Client Agreement.

12.4 TCT may suspend an integration that creates a security, privacy, performance or licensing risk.

13. Protection of personal information

13.1 Users must process personal information through the Services only where:

- The processing is authorised;
- It is necessary for a legitimate purpose;
- The information is relevant to that purpose;
- The User is permitted to provide or access it; and
- The processing complies with the TCT Privacy and Data Protection Policy.

13.2 Users must not:

- Access learner information without a legitimate need;
- Browse learner records out of curiosity;
- Export reports without authority;
- Send reports to unauthorised recipients;
- Upload unnecessary personal information;
- Use learner information for an unrelated purpose;
- Create unauthorised personal databases;
- Disclose personal information publicly;
- Retain downloaded reports longer than necessary; or
- Use TCT information for unauthorised profiling or marketing.

13.3 Administrators must verify recipients before distributing learner reports.

13.4 Downloaded reports must be:

- Stored securely;
- Accessible only to authorised persons;
- Used only for the disclosed purpose;
- Protected during transmission; and
- Deleted when no longer required.

© Business Confidential

13.5 A User who receives personal information in error must:

- Stop reviewing it;
- Avoid copying or sharing it;
- Notify TCT promptly;
- Follow any containment instruction; and
- Delete or return it when instructed.

14. Confidential, regulated and sensitive information

14.1 Users must not enter real confidential, regulated or security-sensitive information into learning activities unless TCT has expressly authorised the use and appropriate safeguards are in place.

14.2 Restricted information includes:

- Customer or merchant personal information;
- Live payment-transaction information;
- Complete payment-card numbers;
- Card verification information;
- PIN information;
- Authentication credentials;
- Cryptographic keys;
- Security codes;
- API secrets;
- Access tokens;
- Production-system passwords;
- Fraud-monitoring case information;
- Suspicious-transaction information;
- Internal vulnerability information;
- Confidential pricing;
- Confidential contracts;
- Non-public financial information;
- Proprietary source code; and
- Information subject to regulatory, legal or contractual restrictions.

14.3 Users should use:

- Fictional information;
- Anonymised information;
- Masked information;
- Synthetic examples; or
- TCT-provided scenarios,

where actual information is not necessary.

14.4 A User must not use a Course, discussion area, support request, simulation or AI Tool as a storage location for confidential business records.

14.5 The accidental submission of restricted information must be reported promptly.

15. Intellectual property and Course Materials

15.1 Course Materials may be accessed only for the authorised User's learning or approved administrative purpose.

15.2 Unless TCT has expressly authorised the activity in writing, Users must not:

- Copy Course Materials;
- Reproduce Course Materials;
- Photograph Course Materials;
- Take screenshots for distribution;
- Screen-record a Course;
- Record audio or video;
- Download content not made available for download;
- Publish Course Materials;
- Upload Course Materials to another system;
- Share Course Materials with unauthorised persons;
- Sell or licence Course Materials;
- Translate or adapt Course Materials;
- Remove copyright or ownership notices;
- Incorporate Course Materials into another course;
- Use Course Materials to train other persons;
- Use Course Materials to build a competing product;
- Submit Course Materials to an external AI system;
- Convert Course Materials into SCORM or another learning format;
- Rebrand or white-label Course Materials; or
- Create a derivative commercial product.

15.3 A download option does not transfer ownership or authorise redistribution.

15.4 Authorised internal use must remain within the scope of the relevant Client Agreement.

15.5 Users must not represent TCT Course Materials as their own work.

15.6 Users may refer to knowledge gained through a Course in their professional work, but may not reproduce protected expression, proprietary frameworks or substantial Course Materials without permission.

16. Certificates and credentials

16.1 Users may share a valid Certificate issued in their own name for legitimate professional purposes.

16.2 Users must not:

- Alter a Certificate;
- Change a learner name;
- Change a Course title;
- Change a completion date;
- Remove verification information;
- Create a false TCT Certificate;
- Use another person's Certificate;
- Misrepresent an incomplete Course as completed;
- Claim accreditation not stated by TCT; or
- Misrepresent the scope of a Certificate.

16.3 A Certificate must not be used to imply:

- Regulatory approval;
- Statutory licensing;
- Professional accreditation;
- Employment suitability;
- TCT endorsement of the User's employer or services; or
- Competence beyond the Course completed.

16.4 Suspected Certificate fraud may result in:

- Verification review;
- Suspension;
- Certificate revocation;
- Notification of a Sponsor;
- Legal action; or
- Referral to an appropriate authority.

17. Assessments and academic integrity

17.1 Users must complete assessments honestly and in accordance with the applicable instructions.

17.2 Users must not:

- Ask another person to complete an assessment;
- Complete an assessment for another person;
- Share assessment questions;
- Share answer keys;
- Copy another learner's work;
- Submit another person's work;

© Business Confidential

- Purchase assessment answers;
- Use unauthorised notes or resources;
- Use AI where prohibited;
- Manipulate completion data;
- Falsify attendance;
- Falsify assessment evidence;
- Exploit repeated attempts to extract an answer bank;
- Publish assessment content online; or
- Assist another person to commit academic misconduct.

17.3 Collaboration is permitted only where the Course instructions expressly allow it.

17.4 Users may discuss general learning concepts but may not disclose protected assessment content.

17.5 Detailed academic-integrity requirements and procedures are contained in the TCT Academic Integrity Policy.

18. Use of AI and automated tools

18.1 Users may use TCT-provided AI Tools only for authorised learning purposes and in accordance with the TCT AI Acceptable Use Policy.

18.2 Users must not use AI or automated tools to:

- Complete a prohibited assessment;
- Impersonate another person;
- Generate false evidence of participation;
- Extract Course Materials;
- Circumvent access controls;
- Generate abusive or unlawful content;
- Process restricted information without authority;
- Make unauthorised decisions about another person;
- Mislead TCT, a facilitator or a Client Organisation;
- Create fraudulent Certificates or records; or
- Develop a competing training product from TCT content.

18.3 AI outputs must not be represented as verified TCT advice unless they have been formally reviewed and approved by TCT.

18.4 Users remain responsible for reviewing and verifying AI-generated information.

18.5 Use of external AI tools with TCT Course Materials is prohibited unless TCT has provided written authorisation.

© Business Confidential

19. Communications and professional conduct

19.1 Users must communicate professionally and respectfully through:

- Discussion forums;
- Virtual sessions;
- Chats;
- Support requests;
- Emails;
- Role-plays;
- Feedback tools;
- Assessments; and
- Other TCT communication channels.

19.2 Users must not submit, publish, display or communicate content that:

- Harasses or threatens another person;
- Is discriminatory;
- Is defamatory;
- Is deliberately humiliating;
- Encourages violence or unlawful conduct;
- Contains unlawful hate speech;
- Contains sexually explicit or exploitative material;
- Invades another person's privacy;
- Discloses confidential information;
- Impersonates another person;
- Is knowingly false or deceptive;
- Contains malicious links;
- Is intended to disrupt learning;
- Is unrelated commercial advertising;
- Constitutes spam; or
- Otherwise materially interferes with the safe and professional use of the Services.

19.3 Reasonable disagreement, constructive criticism and professional debate are permitted.

19.4 Users must not retaliate against a person who:

- Raises a genuine complaint;
- Reports suspected misconduct;
- Requests assistance;
- Exercises a lawful privacy right; or
- Participates in an investigation.

19.5 Facilitators and administrators may moderate or remove content that breaches this Policy.

© Business Confidential

20. Identity, impersonation and misrepresentation

Users must not:

20.1 Impersonate:

- Another learner;
- A TCT employee;
- A facilitator;
- An assessor;
- A Client Organisation representative;
- A regulator;
- A payment scheme;
- A bank;
- A technology provider; or
- Any other person or organisation.

20.2 Misrepresent authority to act for TCT or a Client Organisation.

20.3 Use misleading names, email addresses, job titles or organisational information.

20.4 Create a false impression that TCT endorses a product, service or person.

20.5 Use TCT branding, logos or trade names without authorisation.

20.6 Issue statements, certificates, reports or communications purporting to come from TCT without authority.

21. Commercial and competitive misuse

21.1 The Services may not be used to compete unfairly with TCT or commercially exploit TCT resources.

21.2 Without prior written authorisation, Users must not:

- Resell access;
- Bundle TCT Courses into another service;
- Charge others to access an Account;
- Use TCT content to provide training;
- Build a competing course from TCT Course Materials;
- Copy TCT Course structures or assessments;
- Harvest TCT client or learner information;
- Solicit TCT learners through the Platform;
- Advertise unrelated services;
- Use the Platform for unauthorised recruitment;
- Conduct unauthorised market research;
- Reverse-engineer TCT learning methods; or
- Use demonstration access for competitive intelligence.

© Business Confidential

21.3 Nothing in this clause prevents a User from applying legitimately acquired knowledge in the User's normal work.

22. Unlawful and fraudulent conduct

Users must not use the Services to:

22.1 Commit, facilitate, encourage or conceal unlawful conduct.

22.2 Commit fraud or identity theft.

22.3 Misappropriate information or intellectual property.

22.4 Offer, request or facilitate a bribe or improper advantage.

22.5 Create false payment, training or employment records.

22.6 Circumvent legal, regulatory, risk or compliance controls.

22.7 Launder funds or conceal the source or destination of unlawful funds.

22.8 Facilitate unauthorised access to systems or information.

22.9 Distribute unlawfully obtained information.

22.10 Interfere with an investigation or destroy relevant evidence.

22.11 A User who receives an instruction that appears unlawful or inconsistent with this Policy must not proceed merely because the instruction came from an employer, manager, client or colleague.

23. Virtual sessions and recordings

23.1 Users participating in virtual sessions must:

- Use an appropriate display name;
- Join only sessions for which they are authorised;
- Follow facilitator instructions;
- Avoid unnecessary disclosure of confidential information;
- Behave professionally;
- Protect meeting links; and
- Avoid disrupting the session.

23.2 Users must not record, stream, photograph or capture a facilitated session without prior authorisation.

23.3 Where TCT records a session, participants must be informed where required.

23.4 Authorised recordings may be used only for the communicated purpose.

23.5 Meeting links, access codes and recordings must not be shared with unauthorised persons.

24. Support systems

24.1 Support facilities may be used only for legitimate service-related matters.

24.2 Users must not:

- Submit false incidents;
- Repeatedly submit duplicate requests;
- Abuse support personnel;
- Submit malicious attachments;
- Use support systems for unrelated marketing;
- Demand disclosure of another User's information;
- Attempt to manipulate support staff into bypassing controls; or
- Use support communications to obtain unauthorised access.

24.3 Users should provide sufficient information to allow TCT to investigate a legitimate issue.

24.4 Sensitive Credentials must not be included in a support request unless TCT has expressly requested a secure form of submission.

25. Administrator responsibilities

25.1 Administrators receive elevated access and must exercise additional care.

25.2 An Administrator must:

- Use administrative access only for authorised duties;
- Access only the learners and reports within the Administrator's responsibility;
- Protect administrative Credentials;
- Verify learner information before upload;
- Verify recipients before sending reports;
- Remove access when no longer required;
- Maintain confidentiality;
- Follow Client Agreement restrictions;
- Avoid unnecessary downloads;
- Report suspicious activity;
- Avoid using administrative access for personal benefit; and
- Cooperate with TCT access reviews.

© Business Confidential

25.3 An Administrator must not:

- View learner information without a legitimate reason;
- Alter results without authority;
- Create false completion records;
- Issue unauthorised Certificates;
- Reassign Accounts improperly;
- Conceal seat sharing;
- Export information for unrelated purposes;
- Grant access beyond the organisation's entitlement;
- Share administrative access; or
- Override controls without authority.

25.4 Client Organisations must notify TCT promptly when an Administrator:

- Leaves the organisation;
- Changes role;
- No longer requires access;
- Is subject to a security concern; or
- Should have permissions reduced or removed.

26. Facilitator, assessor and contractor responsibilities

26.1 Facilitators, assessors and contractors must:

- Use access only for assigned duties;
- Maintain learner confidentiality;
- Apply assessment criteria consistently;
- Protect assessment materials;
- Avoid conflicts of interest;
- Use approved communication channels;
- Protect records;
- Report suspected misconduct;
- Avoid retaining unnecessary learner information; and
- Return or delete information when instructed.

26.2 They must not:

- Disclose learner results to unauthorised persons;
- Alter results improperly;
- Favour or disadvantage a learner for an improper reason;
- Share assessment answers;
- Use learner information for private commercial purposes;
- Upload TCT content to unauthorised systems;
- Use TCT access after the assignment ends; or
- Represent personal opinions as official TCT decisions without authority.

© Business Confidential

27. Client Organisation responsibilities

A Client Organisation must:

27.1 Authorise only eligible Users.

27.2 Purchase and maintain sufficient learner capacity or licences.

27.3 Prevent account sharing and unauthorised seat rotation.

27.4 Provide accurate learner and Administrator information.

27.5 Inform Users of this Policy.

27.6 Use learner reports only for lawful and disclosed purposes.

27.7 Protect learner lists, reports and Credentials.

27.8 Remove or update access when a User leaves, changes role, enters extended leave, is affected by an urgent project call-up or otherwise no longer requires access, subject to the Client Agreement.

27.9 Report suspected misuse or security incidents promptly.

27.10 Avoid directing a User to breach this Policy.

27.11 Cooperate with reasonable investigations.

27.12 Ensure that its own systems, integrations and administrators do not compromise TCT Services.

28. Monitoring and audit records

28.1 TCT may monitor and record use of the Services to:

- Administer Accounts;
- Deliver Courses;
- Track progress;
- Verify completion;
- Protect security;
- Detect account sharing;
- Investigate misconduct;
- Protect intellectual property;
- Maintain service quality;
- Generate authorised reports;
- Respond to complaints;
- Enforce agreements; and
- Meet legal obligations.

28.2 Monitoring information may include:

- Login activity;
- IP addresses;
- Device and browser information;
- Session activity;
- Course access;
- Downloads;
- Assessment attempts;
- Learning progress;
- Administrative changes;
- AI Tool interactions;
- Support activity;
- Security events; and
- Unusual usage patterns.

28.3 Monitoring will be conducted in accordance with the TCT Privacy and Data Protection Policy and applicable law.

28.4 Users should not expect personal privacy when using TCT systems for unauthorised purposes, but monitoring will remain proportionate to legitimate operational, security and legal requirements.

28.5 TCT may retain audit records for an appropriate period for:

- Security;
- Contract administration;
- Academic integrity;
- Dispute resolution;
- Certificate verification;
- Legal compliance; and
- Investigation.

29. Reporting suspected misuse

29.1 Users must promptly report:

- Suspected account sharing;
- Unauthorised access;
- Credential compromise;
- Malware;
- Security vulnerabilities;
- Improper disclosure;
- Academic misconduct;
- Certificate fraud;
- Harassment;
- Intellectual-property misuse;
- Suspicious administrative activity;
- Bribery or corruption;

- Fraudulent conduct; or
- Any material breach of this Policy.

29.2 Reports may be submitted to:
Email: legal@transacttraining.online
Subject line: Acceptable Use or Security Report

29.3 A report should include, where available:

- The reporter's name and contact information;
- The Account or organisation involved;
- A description of the concern;
- Relevant dates and times;
- Supporting evidence;
- The affected Course or system; and
- Any immediate risk requiring attention.

29.4 Users must not conduct their own intrusive investigation.

29.5 Evidence must not be obtained through unauthorised access.

29.6 TCT will treat genuine reports as confidential to the extent reasonably possible.

30. Investigation procedures

30.1 TCT may investigate suspected breaches of this Policy.

30.2 An investigation may include:

- Reviewing Platform logs;
- Reviewing Account activity;
- Reviewing downloads;
- Reviewing assessment attempts;
- Reviewing relevant communications;
- Preserving records;
- Requesting information from the User;
- Requesting information from a Client Organisation;
- Temporarily restricting access;
- Interviewing relevant persons;
- Consulting technical providers;
- Conducting a human review of automated alerts; and
- Obtaining professional or legal advice.

30.3 TCT will seek to conduct investigations:

- Fairly;
- Objectively;
- Confidentially;
- Proportionately;
- Without unreasonable delay; and
- In accordance with applicable law.

30.4 A User may be given a reasonable opportunity to respond before a final adverse decision, except where immediate action is required to:

- Protect security;
- Prevent harm;
- Preserve evidence;
- Stop ongoing misuse; or
- Comply with law.

30.5 A refusal to cooperate may be taken into account where cooperation is reasonably required and lawfully requested.

31. Enforcement and consequences

31.1 TCT may take action proportionate to:

- The seriousness of the conduct;
- Whether it was deliberate;
- The harm caused or risk created;
- Whether it was repeated;
- The User's response;
- The need to protect others;
- Contractual requirements; and
- Applicable law.

31.2 Actions may include:

- Informal guidance;
- A warning;
- Required corrective action;
- Password reset;
- Removal of content;
- Restriction of a function;
- Temporary suspension;
- Permanent Account termination;
- Removal from a Course;
- Cancellation of an assessment attempt;
- Reassessment;
- Withholding of results;
- Failure of an assessment or Course;

- Withdrawal or revocation of a Certificate;
- Removal of Administrator privileges;
- Notification of a Client Organisation;
- Recovery of direct loss;
- Termination of a Client Agreement;
- Legal action;
- Reporting to a regulator; or
- Reporting suspected criminal conduct to an appropriate authority.

31.3 TCT may act immediately where a breach creates a material risk to:

- Security;
- Personal information;
- Intellectual property;
- Platform availability;
- Assessment integrity;
- Another User;
- A Client Organisation; or
- TCT's legal obligations.

31.4 A suspension or termination does not remove:

- Payment obligations already incurred;
- Confidentiality duties;
- Intellectual-property restrictions;
- Liability for prior conduct; or
- Record-retention requirements.

31.5 Where a Client Organisation requests suspension or removal of one of its Users, TCT may implement the request where it is consistent with the Client Agreement and applicable law.

32. Complaints and appeals

32.1 A User may challenge an enforcement decision where an appeal is permitted under the TCT Complaints and Appeals Policy.

32.2 An appeal should identify:

- The decision challenged;
- The grounds for the appeal;
- Relevant supporting information;
- Any material procedural concern; and
- The outcome requested.

32.3 An appeal does not automatically suspend a security restriction where continued access could create a material risk.

32.4 Appeals should be considered by a person who was not solely responsible for the original decision where reasonably practicable.

32.5 Nothing in this Policy prevents a person from exercising rights available under law or an applicable Client Agreement.

33. Emergency and protective action

33.1 TCT may take immediate protective action without prior notice where reasonably necessary to:

- Contain a security incident;
- Disable compromised Credentials;
- Stop unauthorised disclosure;
- Preserve evidence;
- Prevent academic fraud;
- Protect intellectual property;
- Protect Platform availability;
- Prevent ongoing harassment;
- Comply with a lawful instruction; or
- Reduce a material risk.

33.2 Protective action may include:

- Blocking access;
- Ending sessions;
- Resetting Credentials;
- Isolating affected information;
- Disabling an integration;
- Restricting downloads;
- Preserving logs;
- Removing content; or
- Temporarily suspending a User or Client environment.

33.3 TCT will review temporary protective action once the immediate risk has been assessed.

34. Exceptions and written permission

34.1 An exception to this Policy is valid only where:

- It is lawful;
- It has a legitimate business or learning purpose;
- Risks have been assessed;
- Appropriate controls are in place; and

© Business Confidential

- It has been approved in writing by an authorised TCT representative.

34.2 An exception must specify:

- The activity authorised;
- The persons authorised;
- The systems or information involved;
- The permitted period;
- Applicable safeguards; and
- Any reporting requirements.

34.3 An exception does not authorise activity outside its stated scope.

34.4 TCT may withdraw an exception where:

- Conditions are breached;
- Risk materially increases;
- The purpose ends;
- The authorisation expires; or
- Continued permission becomes unlawful or unsafe.

35. Policy ownership and responsibilities

35.1 TCT management

TCT management is responsible for:

- Approving this Policy;
- Supporting its implementation;
- Providing appropriate resources;
- Reviewing material incidents;
- Ensuring alignment with Client Agreements; and
- Promoting responsible use.

35.2 Information Officer
The Information Officer is responsible for matters involving personal information and privacy compliance.

35.3 Security responsibility
The person or function responsible for information security must support:

- Security monitoring;
- Incident response;
- Access controls;
- Vulnerability management;
- Technical investigations; and
- Security-awareness activities.

35.4 Course and academic responsibility
The relevant Course, assessment or academic function must support:

- Assessment integrity;
- Facilitator conduct;
- Learner guidance;
- Academic-misconduct processes; and
- Certificate integrity.

35.5 Client Organisations
Client Organisations are responsible for the conduct of their authorised Users and Administrators to the extent set out in the Client Agreement and applicable law.

35.6 Users
Each User is personally responsible for:

- Protecting the User's Account;
- Using the Services appropriately;
- Following instructions;
- Protecting information;
- Avoiding prohibited conduct;
- Reporting suspected breaches; and
- Cooperating with legitimate remedial action.

36. Policy hierarchy

36.1 In the event of a conflict, the following order of precedence applies:

1. Mandatory applicable law;
2. A signed data-processing agreement for personal-information matters;
3. The applicable Master Agreement, Academy Agreement or equivalent Client Agreement;
4. The applicable Order, Schedule or Statement of Work;
5. The TCT Terms of Service;
6. This Acceptable Use Policy;
7. Other applicable TCT policies; and
8. General Course descriptions or guidance.

36.2 A more specific document takes precedence only for the specific matter it addresses.

36.3 No document takes precedence to the extent that it would authorise:

- Unlawful conduct;
- Unauthorised system access;
- Security compromise;
- Fraud;
- Bribery;
- Academic misconduct;

© Business Confidential

- Unlawful processing of personal information; or
- Unauthorised infringement of intellectual property.

37. Changes to this Policy

37.1 TCT may amend this Policy to reflect:

- Changes in law;
- New security risks;
- Technology changes;
- New Platform functionality;
- AI developments;
- New Course formats;
- Changes to Client requirements;
- Lessons from incidents;
- Changes in industry practice; or
- Improvements to TCT governance.

37.2 Each version should display:

- A version number;
- An effective date;
- A last-reviewed date; and
- The responsible policy owner.

37.3 Material changes may be communicated through:

- The TCT website;
- The LMS;
- Email;
- A Client Organisation administrator;
- An updated acceptance notice; or
- Another appropriate channel.

37.4 TCT may require Users to acknowledge or accept an updated version before continuing to use the Services.

38. Contact details
Questions, requests for permission and reports relating to this Policy may be directed to:

Transact Connect Training (Pty) Ltd
Email: legal@transacttraining.online
Subject line: Acceptable Use Policy
Website: www.transacttraining.online
Security concerns should be marked:
Subject line: Urgent Security Report

39. Acknowledgement

By registering for, accessing or using the TCT Platform, Courses, Academies or Services, the User confirms that the User:

- Has been given access to this Policy;
- Understands the acceptable-use requirements;
- Agrees to comply with this Policy;
- Accepts responsibility for activity conducted through the User's Account;
- Understands that use may be monitored for legitimate purposes; and
- Understands that a breach may result in restriction, suspension, termination or other appropriate action.