Privacy & Data Protection Policy

Universal Privacy Notice
Applicable to All Clients, Learners and Authorised Users

Document status: External policy and privacy notice
Policy owner: Transact Connect Training (Pty) Ltd
Version: 1.2
Effective date: 20 January 2025
Last reviewed: 28 July 2026
Next scheduled review: Within 12 months of the effective date
Website: www.transacttraining.online
Privacy contact: legal@transacttraining.online

---

1. Introduction

1.1 Transact Connect Training (Pty) Ltd is committed to protecting personal information and respecting the privacy rights of all persons whose information it processes.

1.2 This Privacy and Data Protection Policy explains how Transact Connect Training collects, receives, records, stores, uses, shares, secures, retains and disposes of personal information.

1.3 Transact Connect Training is referred to in this Policy as:

- **"TCT"**;
- **"we"**;
- **"us"**; or
- **"our."**

1.4 This Policy applies to the processing of personal information through:

- The TCT learning management system;
- TCT websites and web portals;
- TCT online Courses and Academies;
- Assessments and certification;
- AI-enabled learning tools;
- Virtual facilitated sessions;
- Customer and learner support;
- Client and sponsor reporting;
- Sales and client-engagement activities;
- Email and electronic communications;
- Course purchases and billing;
- Surveys and programme evaluations;
- Events, webinars and demonstrations;
- Contract administration;
- Business operations; and
- Related services provided by TCT.

1.5 This Policy must be read together with:

- The TCT Terms of Service;
- The TCT Acceptable Use 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 applicable Course or Academy Order; and
- Any specific privacy notice presented when information is collected.

2. Purpose of this Policy

The purposes of this Policy are to:

2.1 Explain what personal information TCT processes.

2.2 Explain why and how TCT processes personal information.

2.3 Identify the persons and organisations with whom information may be shared.

2.4 Describe how TCT protects personal information.

2.5 Explain how long information may be retained.

2.6 Explain the rights available to data subjects.

2.7 Establish responsibilities for TCT personnel, Client Organisations, administrators, learners and service providers.

2.8 Promote lawful, fair, transparent and responsible information-processing practices throughout TCT's operations.

3. Scope

3.1 This Policy applies to personal information relating to:

- Learners;
- Prospective learners;
- Individual purchasers;
- Client Organisation representatives;
- Client administrators;
- Employer-sponsored learners;
- Sponsors;
- Website visitors;
- Webinar and event participants;
- Facilitators;
- Assessors;
- Consultants;

- Contractors;
- Suppliers;
- Partners;
- Job applicants;
- Employees;
- Former employees;
- Business contacts;
- Shareholders and investors;
- Complainants;
- Enquirers; and
- Any other identifiable person whose information TCT processes.

3.2 This Policy applies to personal information processed:

- Electronically;
- Through the LMS;
- Through email;
- In cloud systems;
- In paper records;
- Through virtual meeting platforms;
- Through AI-enabled systems;
- Through support platforms;
- Through payment and accounting systems; and
- Through third-party service providers acting for or with TCT.

3.3 This Policy applies across all current and future TCT Courses, Academies, learning programmes, products and services.

3.4 This Policy is not limited to any particular Client Organisation.

4. Legal framework

TCT processes personal information in accordance with applicable South African law, including the Protection of Personal Information Act 4 of 2013, commonly known as POPIA, and the Promotion of Access to Information Act 2 of 2000, commonly known as PAIA.

POPIA establishes conditions for lawful processing, including accountability, processing limitation, purpose specification, further-processing limitation, information quality, openness, security safeguards and data-subject participation.

Where TCT provides services outside South Africa or processes information relating to persons in another jurisdiction, additional data-protection laws may apply. TCT will assess those requirements according to the particular processing activity, contract and jurisdiction.

5. Definitions

For purposes of this Policy:

5.1 “Client Agreement”
Means a master services agreement, academy agreement, proposal, order form, schedule, statement of work, data-processing agreement or other written agreement between TCT and a Client Organisation.

5.2 “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.

5.3 “Consent”
Means a voluntary, specific and informed expression of agreement to the processing of personal information.

5.4 “Data Subject”
Means the person or organisation to whom personal information relates.

5.5 “De-identify”
Means removing or altering information so that it cannot reasonably be linked to an identifiable person.

5.6 “Operator”
Means a person or organisation that processes personal information for a responsible party under a contract or mandate without determining the primary purpose of the processing.

5.7 “Personal Information”
Means information relating to an identifiable natural person and, where applicable under South African law, an identifiable juristic person.

5.8 “Processing”
Includes collecting, receiving, recording, organising, storing, updating, retrieving, consulting, using, sharing, transmitting, combining, restricting, deleting and destroying personal information.

5.9 “Responsible Party”
Means the person or organisation that, alone or together with others, determines why and how personal information is processed.

5.10 “Services”
Means the TCT LMS, websites, Courses, Academies, assessments, Certificates, AI-enabled tools, facilitated sessions, support, reporting, professional services and related activities.

© Business Confidential

5.11 “Special Personal Information”
Includes information concerning matters such as health, biometric information, criminal behaviour, religious or philosophical beliefs, political persuasion, race or ethnic origin, trade-union membership and sex life.

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

6. TCT’s data-protection role

6.1 TCT as responsible party
TCT generally acts as the responsible party where it determines the purpose and means of processing for activities including:

- Creating and administering LMS Accounts;
- Managing learner identities;
- Delivering Courses;
- Recording learning progress;
- Administering assessments;
- Issuing and verifying Certificates;
- Providing support;
- Protecting the security of the Platform;
- Maintaining business and financial records;
- Managing complaints and appeals;
- Communicating service information;
- Managing its websites;
- Conducting lawful marketing;
- Improving its Courses and Services;
- Managing its suppliers and personnel; and
- Meeting legal and regulatory obligations.

6.2 TCT as operator
TCT may act as an operator where a Client Organisation determines the primary purpose and essential means of processing and instructs TCT to process information on its behalf.

Examples may include:

- Uploading a client-provided learner list;
- Administering client-specific enrolments;
- Producing reports required by a Client Organisation;
- Hosting Client Organisation content;
- Implementing client-specific learner groupings;
- Processing information under a client-defined training programme; or
- Providing agreed administrative services.

6.3 Client Organisation as responsible party
A Client Organisation may act as a separate responsible party where it:

- Selects learners;
- Provides learner information to TCT;
- Determines why employees must complete training;
- Receives and uses learning reports;
- Makes employment, performance, capability or compliance decisions;
- Determines internal access rights; or
- Combines TCT reports with its own employee or business information.

6.4 Determining the applicable role
The actual role of TCT and a Client Organisation is determined by the facts, purposes and decision-making authority involved in the particular processing activity, not merely by the terminology used in an agreement.

6.5 Joint activities
Where TCT and another party jointly determine a processing activity, their respective responsibilities should be recorded in an appropriate agreement or data-processing arrangement.

7. Data-protection principles
TCT will apply the following principles when processing personal information:

7.1 Accountability
TCT will take reasonable steps to ensure that its processing activities comply with this Policy and applicable law.

7.2 Lawfulness and fairness
Personal information will be processed lawfully, reasonably and in a manner that does not unjustifiably infringe privacy.

7.3 Purpose limitation
Personal information will be collected for specific, defined and legitimate purposes.

7.4 Minimality
TCT will seek to collect only information that is adequate, relevant and reasonably necessary for the applicable purpose.

7.5 Further-processing compatibility
Information will not be used for a materially incompatible purpose unless:

- The further processing is permitted by law;
- The Data Subject has agreed where consent is required;
- The information has been appropriately de-identified; or
- Another lawful justification applies.

7.6 Information quality
TCT will take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.

7.7 Openness
TCT will provide appropriate information about its processing practices through this Policy, collection notices, contractual terms and other communications.

7.8 Security safeguards
TCT will maintain reasonable technical and organisational safeguards appropriate to the nature of the information and the relevant risks.

7.9 Data-subject participation
TCT will provide reasonable mechanisms through which Data Subjects may exercise applicable rights.

These principles reflect the conditions for lawful processing set out in POPIA.

8. Categories of personal information

Depending on the relationship and Service involved, TCT may process the following categories of information.

8.1 Identity information
This may include:

- Full name and surname;
- Preferred name;
- Username;
- Learner or employee identifier;
- Identity verification information;
- Signature;
- Photograph; and
- Date of birth where reasonably required.

8.2 Contact information
This may include:

- Business email address;
- Personal email address;
- Telephone number;
- Physical or postal address;
- Country;
- Region;
- Time zone; and
- Communication preferences.

8.3 Employment and organisational information
This may include:

- Employer;
- Role or job title;
- Department;
- Business unit;

- Seniority level;
- Manager;
- Organisational region;
- Staff number;
- Professional responsibilities; and
- Sponsoring organisation.

8.4 Account and authentication information
This may include:

- Username;
- Encrypted or securely managed password information;
- Account status;
- Activation records;
- Authentication events;
- Multi-factor authentication information;
- Access permissions; and
- Administrator status.

TCT does not ordinarily have access to a User's readable password where passwords are managed securely by the Platform.

8.5 Learning and assessment information
This may include:

- Course enrolments;
- Learning pathways;
- Module and unit activity;
- Progress percentage;
- Completion status;
- Time spent;
- Assessment answers;
- Assessment results;
- Number of attempts;
- Facilitator feedback;
- Attendance;
- Role-play activity;
- Simulation activity;
- Academic-integrity records;
- Course evaluations;
- Certificates;
- Certificate identifiers; and
- Credential-verification records.

8.6 Technical and usage information
This may include:

- IP address;
- Browser type;
- Device information;
- Operating system;
- Session information;
- Login history;
- Pages or Course areas accessed;
- Downloads;
- Error records;
- System logs;
- Security events;
- Cookie identifiers;
- Approximate location derived from technical information; and
- Platform-performance data.

8.7 Communication and support information
This may include:

- Emails;
- Support requests;
- Complaints;
- Appeals;
- Chat messages;
- Survey responses;
- Meeting notes;
- Call records;
- Virtual-session participation;
- Feedback;
- Enquiries; and
- Related correspondence.

8.8 Commercial and transaction information
This may include:

- Courses or Services purchased;
- Proposal information;
- Contract information;
- Invoice information;
- Payment status;
- Billing address;
- Transaction references;
- Tax information;
- Discount arrangements; and
- Procurement information.

TCT should not ordinarily retain complete payment-card credentials where payment is processed by an authorised payment service provider.

8.9 Marketing and relationship information
This may include:

- Business interests;
- Course interests;
- Event attendance;
- Campaign responses;
- Communication preferences;
- Lead source;
- Sales engagement;
- Proposal history; and
- Opt-in or opt-out records.

8.10 AI interaction information
This may include:

- Prompts;
- AI-generated responses;
- Scenario selections;
- Role-play activity;
- User feedback;
- Safety events;
- Usage metadata; and
- Information required to administer and improve an AI-enabled learning activity.

8.11 Supplier, contractor and personnel information
This may include:

- Qualifications;
- Professional history;
- Contract information;
- Banking information;
- Tax information;
- Performance information;
- Access permissions;
- Confidentiality obligations; and
- Due-diligence information.

9. Sources of personal information

TCT may collect or receive personal information from:

9.1 The Data Subject directly.

9.2 A Client Organisation, employer or Sponsor.

9.3 An authorised organisational administrator.

9.4 A manager, facilitator, assessor or support representative.

9.5 A person who purchases or arranges training for someone else.

9.6 The TCT LMS and associated technical systems.

9.7 TCT websites, forms, surveys and event-registration systems.

9.8 Payment processors, accounting systems and financial institutions.

9.9Service providers supporting TCT's operations.

9.10 Publicly available professional and business sources.

9.11 A recruitment agency, referee or previous employer where legally permitted.

9.12 Government, regulatory or law-enforcement bodies where legally authorised.

9.13 Other sources where the Data Subject has authorised the disclosure or the collection is otherwise lawful.

10. Purposes of processing

TCT may process personal information for the following purposes.

10.1 Account creation and administration
To:

- Register Users;
- Create Accounts;
- Authenticate access;
- Manage permissions;
- Update Account information;
- Prevent duplicate or fraudulent Accounts; and
- Administer deactivation or reassignment.

© Business Confidential

10.2 Course and Academy delivery
To:

- Enrol learners;
- Allocate Courses;
- Present Course Materials;
- Track progress;
- Provide learning support;
- Facilitate virtual sessions;
- Administer learning pathways; and
- Manage access periods.

10.3 Assessment and certification
To:

- Administer assessments;
- Record results;
- Verify learner identity;
- Detect academic misconduct;
- Issue Certificates;
- Maintain credential records; and
- Verify Certificates when reasonably requested.

10.4 Sponsored-learning administration
To:

- Confirm enrolment;
- Report progress;
- Report assessment and completion information;
- Manage learner capacity;
- Support organisational learning programmes;
- Provide programme-level analytics; and
- Meet Client Agreement requirements.

10.5 AI-enabled learning
To:

- Deliver role-plays;
- Provide simulations;
- Support knowledge exploration;
- Generate learning feedback;
- Administer AI-enabled activities;
- Investigate misuse;
- Protect safety and security; and
- Improve the learning experience using appropriately controlled information.

© Business Confidential

10.6 Customer, learner and technical support
To:

- Respond to questions;
- Resolve access issues;
- Investigate errors;
- Manage complaints;
- Administer appeals;
- Communicate service updates; and
- Maintain support records.

10.7 Security and fraud prevention
To:

- Protect Accounts;
- Detect unauthorised use;
- Investigate account sharing;
- Prevent fraud;
- Monitor suspicious activity;
- Maintain audit records;
- Protect Course Materials; and
- Respond to security incidents.

10.8 Business and contract administration
To:

- Prepare proposals;
- Conclude agreements;
- Administer orders;
- Manage client relationships;
- Invoice and collect payment;
- Manage suppliers;
- Maintain business records;
- Conduct audits; and
- Exercise contractual rights.

10.9 Legal and regulatory compliance
To:

- Meet statutory obligations;
- Respond to lawful requests;
- Maintain required records;
- Establish, exercise or defend legal claims;
- Cooperate with regulators;
- Conduct compliance reviews; and
- Prevent unlawful conduct.

10.10 Service development and quality improvement
To:

- Evaluate Course effectiveness;
- Improve Course Materials;
- Analyse User experience;
- Develop new learning products;
- Correct technical issues;
- Conduct quality assurance;
- Produce de-identified or aggregated analytics; and
- Improve accessibility and support.

10.11 Communications and marketing
To:

- Send service-related communications;
- Communicate Course information;
- Share relevant TCT updates;
- Invite persons to events or webinars;
- Respond to enquiries;
- Manage communication preferences; and
- Conduct lawful direct marketing.

10.12 Recruitment and personnel administration
To:

- Process applications;
- Conduct appropriate checks;
- Manage employment and contractor relationships;
- Administer access;
- Manage performance;
- Meet labour and tax obligations; and
- Protect TCT's legitimate business interests.

11. Lawful grounds for processing

TCT will rely on an appropriate lawful basis for each processing activity. Depending on the circumstances, TCT may process personal information where:

11.1 The Data Subject has provided valid consent.

11.2 Processing is necessary to conclude or perform a contract with the Data Subject.

11.3 Processing is necessary to implement actions requested by the Data Subject before entering into a contract.

11.4 Processing is necessary to comply with a legal obligation.

11.5 Processing protects a legitimate interest of the Data Subject.

11.6 Processing is necessary for TCT or a third party to pursue a legitimate interest, provided that the Data Subject's rights and reasonable expectations are properly considered.

11.7 Processing is required for the proper performance of a public-law duty by a public body.

11.8 Another lawful justification under applicable law applies.

11.9 Where consent is relied upon, the Data Subject may withdraw consent, subject to:

- Processing already lawfully completed;
- Contractual consequences;
- Legal-retention requirements; and
- Other lawful grounds that may continue to apply.

11.10 TCT will not describe every processing activity as being based on consent where another lawful basis is more appropriate.

12. Mandatory and voluntary information

12.1 Certain information is required to:

- Create an Account;
- Verify identity;
- Enrol a learner;
- Deliver a Course;
- Record completion;
- Issue a Certificate;
- Provide support;
- Enter into a contract;
- Process payment; or
- Meet legal obligations.

12.2 Where required information is not provided, TCT may be unable to:

- Register the User;
- Grant access;
- Deliver the relevant Service;
- Complete a transaction;
- Issue a Certificate;
- Resolve a support request; or
- Meet a Client Agreement requirement.

12.3 Optional information will be identified where reasonably practical.

13. Sponsored learners and organisational reporting

13.1 Where training is purchased, arranged or sponsored by a Client Organisation, TCT may provide authorised representatives of that organisation with learner information.

13.2 The information provided may include:

- Learner name;
- Business email address;
- Employer;
- Role;
- Department;
- Course enrolment;
- Account-activation status;
- Progress percentage;
- Module or unit completion;
- Assessment results;
- Assessment attempts;
- Attendance;
- Participation;
- Completion status;
- Certificate information;
- Access-expiry information;
- Academic-integrity outcomes;
- Administrative issues; and
- Information reasonably required to administer the learning programme.

13.3 Reporting will be limited to information reasonably relevant to the applicable programme, Client Agreement and disclosed purpose.

13.4 A Sponsor may use learner information for legitimate purposes including:

- Training administration;
- Skills development;
- Capability management;
- Compliance monitoring;
- Workforce planning;
- Programme evaluation; and
- Verification of Course completion.

13.5 A Client Organisation is independently responsible for ensuring that its use of learner reports is lawful, fair and consistent with its own employee and privacy obligations.

13.6 TCT will not ordinarily share the following with a Sponsor unless lawfully justified:

- Learner passwords;
- Private payment details;
- Unrelated personal information;
- Unnecessary private support communications;
- Detailed AI conversations unrelated to programme administration;
- Special Personal Information not required for the programme; or
- Information exceeding the agreed or disclosed purpose.

13.7 TCT may share information relating to security, fraud, academic misconduct or serious policy breaches where the disclosure is necessary, proportionate and permitted by law or contract.

14. Aggregated and de-identified information

14.1 TCT may aggregate or de-identify information for purposes including:

- Learning analytics;
- Course improvement;
- Benchmarking;
- Research;
- Reporting;
- Product development;
- Service planning; and
- Business analysis.

14.2 TCT will take reasonable steps to ensure that information described as de-identified cannot reasonably be re-identified.

14.3 TCT will not deliberately attempt to re-identify properly de-identified information unless:

- Required for security testing;
- Required to verify the effectiveness of de-identification;
- Authorised by law; and
- Subject to appropriate controls.

15. AI, profiling and automated processing

15.1 TCT may use AI and automated systems to:

- Provide learning feedback;
- Generate role-play responses;
- Support simulations;
- Recommend learning content;
- Identify technical issues;

- Analyse learning activity;
- Detect unusual Account or assessment patterns;
- Assist with support; and
- Produce administrative insights.

15.2 AI-generated information may be inaccurate or incomplete and should not be treated as a final professional, legal, regulatory or employment decision.

15.3 TCT will not ordinarily make a decision that has a significant legal or similarly substantial effect on a person solely through automated processing without:

- A lawful basis;
- Appropriate safeguards;
- An opportunity for meaningful human review where required; and
- An appropriate mechanism for the person to challenge the outcome.

15.4 Final decisions concerning:

- Academic misconduct;
- Certificate revocation;
- Formal complaints;
- Appeals;
- Serious access restrictions; or
- Similar adverse outcomes,

should involve appropriate human review.

15.5 Users must not enter confidential, payment, authentication, customer or security-sensitive information into an AI Tool unless TCT has expressly authorised that processing and appropriate safeguards are in place.

15.6 Further requirements are contained in the TCT AI Acceptable Use Policy.

16. Special Personal Information

16.1 TCT does not ordinarily require Special Personal Information from learners to provide its standard learning Services.

16.2 TCT may process Special Personal Information where:

- The processing is necessary and lawful;
- The Data Subject has provided valid consent where appropriate;
- The processing is necessary to establish, exercise or defend a right or obligation in law;
- The information is required to provide a reasonable accommodation;
- The Data Subject has deliberately made the information public;
- Another statutory authorisation applies; or
- Approval or authorisation has been obtained where required.

16.3 Examples may include:

- Accessibility or disability information required to provide an accommodation;
- Health information relevant to participation arrangements;
- Biometric information used for authorised identity verification;
- Criminal-behaviour information relevant to a lawful investigation; or
- Demographic information collected for an authorised and clearly disclosed purpose.

16.4 Access to Special Personal Information will be restricted to persons with a legitimate need to process it.

16.5 TCT will not use Special Personal Information for unrelated profiling, discrimination or marketing.

The Information Regulator publishes specific guidance concerning the processing of Special Personal Information.

17. Personal information of children

17.1 TCT's standard professional Courses are generally intended for adults.

17.2 TCT will not knowingly enrol or process the information of a child unless:

- Participation has been authorised by TCT;
- The Course or Service is appropriate;
- The processing is permitted by law;
- Any required consent from a competent person has been obtained;
- Appropriate safeguards are implemented; and
- The information collected is limited to what is reasonably necessary.

17.3 A Client Organisation must not submit the personal information of a child to TCT without prior disclosure to TCT and confirmation that the processing is lawful.

17.4 TCT may request evidence of age, authority or consent where reasonably necessary.

17.5 Where TCT becomes aware that a child's information has been collected without an appropriate lawful basis, TCT may restrict, delete or otherwise remediate the processing.

The Information Regulator publishes specific guidance concerning the processing of personal information of children.

18. Cookies and similar technologies

18.1 TCT websites and Platforms may use cookies, pixels, local storage and similar technologies.

18.2 These technologies may be used for:

- Authentication;
- Session management;
- Security;
- User preferences;
- Platform functionality;
- Performance monitoring;
- Analytics;
- Error detection;
- Course delivery; and
- Lawful marketing.

18.3 Cookies may be:

- Strictly necessary;
- Functional;
- Performance-related;
- Analytical; or
- Marketing-related.

18.4 Where required, Users will be given an opportunity to manage non-essential cookie preferences.

18.5 Disabling certain cookies may affect Platform functionality.

18.6 Additional information may be provided through a cookie notice or consent-management tool.

19. Direct marketing

19.1 TCT may communicate information about Courses, events, services and relevant industry learning opportunities where permitted by law.

19.2 Electronic direct marketing will be conducted on an appropriate lawful basis and in accordance with applicable consent, existing-customer and opt-out requirements.

19.3 Marketing communications will identify TCT and provide a reasonable method to unsubscribe or object.

19.4 A person may opt out of marketing without losing access to necessary service communications.

© Business Confidential

19.5 Service communications may continue where required to:

- Administer an Account;
- Deliver a Course;
- Provide security information;
- Communicate policy changes;
- Manage a transaction;
- Issue a Certificate; or
- Meet contractual or legal obligations.

The Information Regulator's guidance distinguishes direct-marketing requirements from necessary operational and service communications.

20. Sharing personal information

TCT may share personal information with the following categories of recipients where reasonably necessary and lawful.

20.1 Client Organisations and Sponsors
For learner administration, reporting, programme evaluation, compliance monitoring and Client Agreement purposes.

20.2 LMS and technology providers
For Platform hosting, account management, technical support, security and Course delivery.

20.3 Cloud and data-hosting providers
For storage, backup, resilience and operational support.

20.4 Communication providers
For email, messaging, webinars, virtual meetings and support communications.

20.5 AI and learning-technology providers
For authorised AI-enabled learning, simulations, feedback and Platform functionality.

20.6 Payment and financial-service providers
For payment processing, billing, fraud prevention and reconciliation.

20.7 Professional advisers
Including lawyers, accountants, auditors, insurers and consultants where reasonably necessary.

20.8 Regulators and public authorities
Where disclosure is required or authorised by law.

20.9 Law-enforcement bodies
Where disclosure is lawfully required, necessary to protect rights or required to investigate suspected unlawful conduct.

20.10 Business transaction participants
In connection with a lawful merger, investment, restructuring, financing, sale or transfer, subject to confidentiality and data-protection safeguards.

20.11 Other recipients
Where:

- The Data Subject has authorised the disclosure;
- The disclosure is necessary to perform a contract;
- The disclosure protects a legitimate interest;
- The information has been appropriately de-identified; or
- Another lawful ground applies.

20.12 TCT does not sell personal information to advertisers or data brokers.

21. Operators and service providers

21.1 TCT may appoint operators and service providers to process personal information on its behalf.

21.2 TCT will take reasonable steps to ensure that material operators:

- Process information only for authorised purposes;
- Maintain appropriate confidentiality;
- Implement reasonable security safeguards;
- Assist with security incidents;
- Delete or return information when required;
- Restrict unauthorised subcontracting; and
- Comply with applicable contractual and legal requirements.

21.3 Where TCT acts as an operator for a Client Organisation, TCT will process personal information according to:

- The Client Agreement;
- Documented lawful instructions;
- Applicable data-protection law; and
- TCT's own security and governance requirements.

21.4 TCT will inform the relevant responsible party of a suspected security compromise affecting information processed on that party's behalf as required by contract and law.

22. Cross-border processing

22.1 TCT may use service providers or systems located outside South Africa.

22.2 Personal information may therefore be stored, accessed or processed in another country.

22.3 TCT will permit cross-border processing only where an appropriate lawful basis and safeguard exists, which may include:

- A law or binding agreement providing an adequate level of protection;
- Contractual obligations requiring appropriate data protection;
- The Data Subject's consent where valid and appropriate;
- Processing necessary for the performance of a contract;
- Processing necessary for the benefit of the Data Subject; or
- Another lawful basis under applicable law.

22.4 TCT will consider:

- The nature of the information;
- The purpose of the transfer;
- The recipient;
- Security arrangements;
- Contractual safeguards;
- Applicable foreign law; and
- The risks to Data Subjects.

22.5 Client Organisations must inform TCT of any specific data-location or transfer restrictions before Services are implemented.

Cross-border processing will be managed in accordance with the applicable requirements of POPIA.

23. Information retention

23.1 TCT will not retain personal information for longer than reasonably necessary for the purpose for which it was collected, unless:

- Retention is required or authorised by law;
- Retention is required by a Client Agreement;
- TCT reasonably requires the record for lawful business purposes;
- The record is required to establish, exercise or defend a legal claim;
- The Data Subject has consented to longer retention; or
- The information has been appropriately de-identified.

23.2 Retention periods may differ according to the information and purpose involved.

23.3 TCT's retention approach may include the following.

Learner Account information
Retained for the duration of access and for an appropriate period afterwards to support administration, reporting, security and dispute resolution.

Learning and completion records
Retained for an appropriate period to verify learning history, completion and programme reporting.

Certificate records
May be retained for an extended period to permit Certificate verification and preserve the integrity of issued credentials.

Assessment records
Retained for an appropriate period to support result verification, academic-integrity investigations, appeals and Client Agreement requirements.

Client and contract records
Retained for the duration of the relationship and for the period required for contractual, financial, tax, audit and legal purposes.

Financial records
Retained for the period required under applicable tax, accounting and corporate law.

Security logs
Retained for a period appropriate to security monitoring, incident investigation, fraud prevention and legal requirements.

Marketing records
Retained while there is a lawful marketing relationship or until the person objects or opts out, subject to maintaining a suppression record.

Complaints and appeals
Retained for an appropriate period to administer the matter, evidence the outcome and manage related risks.

Unsuccessful enquiries and proposals
Retained for a limited period according to legitimate business need, legal obligations and reasonable expectations.

23.4 When information is no longer required, TCT will:

- Securely delete it;
- Destroy it;
- De-identify it; or
- Restrict its processing where deletion is not yet appropriate.

23.5 Deletion or destruction should be conducted in a manner reasonably designed to prevent reconstruction in an intelligible form.

24. Information security

24.1 TCT will implement reasonable technical and organisational measures appropriate to:

- The sensitivity of the information;
- The volume of information;
- The processing purpose;

- The technology used;
- The likelihood of harm;
- The cost and availability of safeguards; and
- Applicable legal and industry requirements.

24.2 Security measures may include:

- Role-based access controls;
- Unique User Accounts;
- Password controls;
- Multi-factor authentication where appropriate;
- Encryption in transit;
- Encryption at rest where appropriate;
- Secure backups;
- Logging and monitoring;
- Anti-malware controls;
- Patch and vulnerability management;
- Secure configuration;
- Access reviews;
- Confidentiality undertakings;
- Personnel training;
- Supplier due diligence;
- Incident-response procedures;
- Business-continuity arrangements;
- Data minimisation;
- Secure deletion;
- Physical safeguards; and
- Periodic risk assessments.

24.3 TCT will limit access to personal information to persons who require it for authorised duties.

24.4 TCT personnel and contractors with access to personal information must:

- Maintain confidentiality;
- Follow TCT policies;
- Use approved systems;
- Protect authentication information;
- Report incidents;
- Avoid unauthorised copying; and
- Complete relevant awareness or training activities.

24.5 No system can be guaranteed to be completely secure. TCT will nevertheless take reasonable and proportionate steps to reduce foreseeable risks.

24.6 Users and Client Organisations must comply with the TCT Information Security Policy and Acceptable Use Policy.

25. Security compromises and personal-information incidents

25.1 A security compromise may include:

- Unauthorised access;
- Accidental disclosure;
- Loss of a device or record;
- Credential compromise;
- Malware;
- Unauthorised alteration;
- Unauthorised deletion;
- Account takeover;
- Misdelivery of information;
- Improper sharing;
- Loss of availability; or
- Any other unauthorised acquisition or access to personal information.

25.2 All Users, personnel, contractors and Client Organisations must promptly report suspected personal-information incidents to TCT.

25.3 TCT will:

- Record and assess the incident;
- Take reasonable containment measures;
- Preserve relevant evidence;
- Investigate the cause and impact;
- Take remediation measures;
- Inform affected Client Organisations where appropriate;
- Notify the Information Regulator where required;
- Notify affected Data Subjects where required;
- Cooperate with lawful investigations; and
- Review controls after the incident.

25.4 Where TCT acts as an operator, TCT will notify the responsible party without undue delay in accordance with the applicable agreement and law.

25.5 Notifications may be delayed only where permitted by law or directed by an authorised public body responsible for the prevention, detection or investigation of offences.

The Information Regulator has stated that POPIA does not prescribe a risk threshold below which a responsible party may disregard its notification obligation following a security compromise.

© Business Confidential

26. Data-subject rights
Subject to applicable law and any lawful limitations, a Data Subject may have the right to:

26.1 Be informed
Receive information about the collection and use of personal information.

26.2 Request access
Ask whether TCT holds personal information about the Data Subject and request access to that information.

26.3 Request correction
Ask TCT to correct or update information that is inaccurate, incomplete, misleading or out of date.

26.4 Request deletion or destruction
Ask TCT to delete or destroy information that TCT is no longer authorised to retain, subject to legal, contractual and legitimate-retention requirements.

26.5 Request restriction
Ask TCT to restrict processing in circumstances recognised by law.

26.6 Object to processing
Object, on reasonable grounds, to certain processing based on legitimate interests or another applicable ground.

26.7 Object to direct marketing
Object at any time to processing for direct-marketing purposes.

26.8 Withdraw consent
Withdraw consent where consent is the basis for processing.

26.9 Challenge automated decisions
Request appropriate review of a qualifying decision made solely through automated processing.

26.10 Complain
Submit a complaint to TCT and, where appropriate, to the Information Regulator.

26.11 Exercise rights without retaliation
Exercise privacy rights without being subjected to retaliation, although lawful consequences may follow where required information cannot be processed.

POPIA provides for Data Subject participation, including rights relating to access and correction of personal information.

© Business Confidential

27. Exercising privacy rights

27.1 Requests may be submitted to:
Email: legal@transacttraining.online
Subject line: Privacy Request

27.2 A request should include:

- The requester's full name;
- Relevant contact details;
- The nature of the relationship with TCT;
- The Account, Client Organisation or Course involved;
- A clear description of the request; and
- Any information reasonably required to locate the relevant records.

27.3 TCT may request reasonable evidence of identity and authority before disclosing, correcting or deleting information.

27.4 Where a request is made on behalf of another person, TCT may require proof of authority.

27.5 TCT will respond within the period required by applicable law.

27.6 A request may be refused or limited where:

- TCT cannot verify identity or authority;
- Disclosure would adversely affect another person's rights;
- The information is legally privileged;
- Retention is required by law;
- The request is manifestly unfounded or excessive;
- Access is governed by PAIA;
- Disclosure would compromise security;
- Another lawful ground for refusal applies; or
- TCT is acting only as an operator and must refer the request to the responsible party.

27.7 Where TCT acts as an operator, it will reasonably assist the Client Organisation in responding to a valid request, subject to the Client Agreement.

27.8 TCT may keep a record of privacy requests and responses for accountability and dispute-resolution purposes.

28. Accuracy and User responsibilities

28.1 Users must provide accurate, complete and current information.

28.2 Users must promptly update information through the Platform or notify TCT or the relevant Client Organisation administrator.

© Business Confidential

28.3 A User must not provide another person's information without authority.

28.4 Client Organisations must take reasonable steps to ensure that learner lists and reporting information supplied to TCT are accurate and lawfully obtained.

28.5 TCT is not responsible for an error caused solely by inaccurate information provided by a User or Client Organisation, but will take reasonable steps to correct the record once notified.

29. Client Organisation responsibilities

A Client Organisation that provides information to TCT or receives learner information must:

29.1 Have an appropriate lawful basis for the processing.

29.2 Inform its employees, contractors or learners about the processing.

29.3 Provide only information reasonably necessary for the programme.

29.4 Ensure that learner information is accurate.

29.5 Restrict administrator and reporting access to authorised persons.

29.6 Use TCT reports only for legitimate and disclosed purposes.

29.7 Protect downloaded reports and learner lists.

29.8 Avoid sending unnecessary sensitive or confidential information.

29.9 Notify TCT when an administrator or learner should no longer have access.

29.10 Report suspected privacy or security incidents promptly.

29.11 Comply with applicable employment, privacy and data-protection obligations.

29.12 Not instruct TCT to process information unlawfully.

29.13 Maintain any records, notices, assessments or consents required for its own processing activities.

30. Personnel, facilitators and contractors

30.1 TCT personnel, facilitators, assessors and contractors may access personal information only where reasonably required for their authorised functions.

30.2 They must:

- Maintain confidentiality;
- Follow approved procedures;
- Use information only for authorised purposes;
- Protect devices and credentials;
- Avoid unauthorised downloads;
- Report incidents;
- Complete required training; and
- Return or securely dispose of information when instructed.

30.3 Access may be withdrawn when a person changes role, leaves TCT or no longer requires access.

30.4 Breaches may result in disciplinary, contractual, legal or other appropriate action.

31. Access to records under PAIA

31.1 A request for access to a record that falls under PAIA may need to be submitted under TCT's PAIA process or PAIA Manual.

31.2 Privacy requests under POPIA and access-to-record requests under PAIA may overlap but are not always identical.

31.3 TCT may require the requester to use the prescribed process or form where applicable.

31.4 Nothing in this Policy limits a right of access available under PAIA.
PAIA provides a mechanism for requesting access to information held by another person where the information is required for the exercise or protection of rights.

32. Complaints

32.1 Internal complaint
A person who believes that TCT has processed personal information unlawfully or unfairly should submit a complaint to:

Email: legal@transacttraining.online
Subject line: Privacy Complaint

32.2 The complaint should include:

- The complainant's name;
- Contact information;
- A description of the concern;
- Relevant dates;
- The Course, Client Organisation or Service involved;

- Supporting information; and
- The outcome sought.

32.3 TCT will:

- Acknowledge the complaint;
- Assess the matter;
- Request further information where required;
- Investigate reasonably;
- Protect confidentiality as far as reasonably possible;
- Communicate an outcome; and
- Take appropriate corrective action where necessary.

32.4 Complaint to the Information Regulator
A Data Subject may lodge a complaint with the Information Regulator if the person believes that personal information has been processed in violation of POPIA.

Current complaint procedures and contact channels should be obtained from the Information Regulator's official website.

32.5 TCT will not retaliate against a person for raising a genuine privacy concern or exercising a lawful right.

33. Policy governance

33.1 The TCT Information Officer is responsible for overseeing this Policy, subject to the responsibilities of TCT's directors and management.

33.2 The Information Officer's responsibilities include:

- Promoting compliance;
- Overseeing privacy requests;
- Supporting incident response;
- Maintaining relevant documentation;
- Reviewing processing activities;
- Supporting awareness and training;
- Managing regulator engagement; and
- Coordinating policy review.

33.3 TCT may appoint Deputy Information Officers or other responsible personnel.

33.4 TCT will maintain appropriate records of:

- Material processing activities;
- Operators;
- Security incidents;
- Privacy requests;
- Complaints;
- Cross-border processing;
- Policy approvals; and

- Relevant assessments and decisions.

33.5 Material new processing activities should be assessed for privacy, security and legal risk before implementation.

34. Changes to this Policy

34.1 TCT may update this Policy to reflect:

- Changes in law or regulatory guidance;
- New Courses or Services;
- New technology;
- AI developments;
- Security requirements;
- New service providers;
- Changes in business operations;
- Lessons from incidents or complaints; or
- Improved governance practices.

34.2 Each published version should display:

- A version number;
- An effective date; and
- A last-reviewed date.

34.3 Material changes may be communicated through:

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

34.4 Where required, TCT may request renewed acknowledgement or consent.

34.5 The version in effect at the time of the relevant processing will apply, subject to applicable law and contractual rights.

35. Relationship with other agreements and policies

35.1 This Policy applies together with the TCT Terms of Service and all applicable TCT policies.

35.2 Where a Client Agreement or data-processing agreement contains more specific privacy provisions, those provisions apply to the specific processing activity addressed in that agreement.

35.3 The following order of precedence applies in the event of a conflict:

1. Mandatory applicable law;
2. A signed data-processing agreement for the specific processing concerned;
3. The applicable Master Agreement, Academy Agreement or equivalent Client Agreement;
4. The applicable Order, Schedule or Statement of Work;
5. This Privacy and Data Protection Policy;
6. The TCT Terms of Service; and
7. Other relevant TCT policies and notices.

35.4 A more specific document takes precedence only in relation to the particular matter it addresses.

35.5 No agreement may authorise processing that is unlawful.

36. Contact details
Questions, requests and complaints relating to this Policy may be directed to:

Transact Connect Training (Pty) Ltd
Email: legal@transacttraining.online

37. Acknowledgement

By registering for, accessing or using the TCT LMS, Courses, Academies or Services, the User acknowledges that the User has been given access to this Privacy and Data Protection Policy and understands how TCT may process personal information.

Acknowledgement of this Policy does not replace consent where consent is specifically required by law, and it does not prevent TCT from relying on another lawful basis where appropriate.