Data Classification Policy

1. Purpose

This policy defines how Subcontext classifies data and the controls applied at each classification level. Classifying data consistently means everyone handling it knows how sensitive it is, who may see it, how it must be protected and how long it may be kept. It underpins the Information Security Policy, the Access Control Policy, the Encryption & Key Management Policy and the Data Retention & Deletion Policy, which each rely on the levels set out here.

2. Scope

This policy applies to:

- All data Subcontext creates, collects, receives or stores, in any form, including data in the platform's database, file storage, cache, logs, backups, exports, source code, email and documents
- Data Subcontext processes on behalf of customers (as a processor) and data it holds for its own purposes (as a controller), such as platform user accounts, billing records, and sales and marketing contacts
- Everyone who handles Subcontext data: directors, employees, contractors and anyone else given access, referred to in this policy as "staff"
- Systems operated by Subcontext and, through contract, the sub-processors on the published Sub-Processor List

3. Definitions

Term	Meaning
Customer	An organisation that subscribes to Subcontext, typically a UK insurer, broker or other regulated firm
Customer data	Any data a customer, or its own customers, puts into or generates on the platform, including contacts, conversations, call recordings, applications, policies, claims, agent configurations and knowledge content
Data owner	The person accountable for a set of data and for deciding its classification. For customer data, this is the customer as controller; within Subcontext, it is the member of the founding team responsible for the system or process
Data handler	Anyone who creates, accesses, moves or deletes data
Need-to-know	Access limited to people whose role requires the data to perform a specific task
Restricted data	Data whose disclosure would directly allow access to other data or systems, such as keys and credentials

4. Classification Levels

Level	Description	Examples
Public	Information intended for public disclosure	Marketing content, public documentation, published legal documents
Internal	Information for internal use that is not sensitive	Internal process documents, meeting notes, non-sensitive operational data
Confidential	Sensitive business or customer information	Customer conversation data, contact information, Agent configurations, API keys, billing data
Restricted	Highly sensitive data requiring the strongest controls	Encryption keys, authentication secrets, integration credentials, database passwords

4.1 Impact if disclosed

The level reflects the harm that unauthorised disclosure, alteration or loss could cause:

Level	Impact
Public	None. The information is already, or is intended to be, freely available
Internal	Minor. Limited inconvenience or embarrassment, no harm to individuals
Confidential	Significant. Harm or distress to individuals, breach of customer contracts or regulatory obligations, reputational damage
Restricted	Severe. Could give an attacker access to large volumes of Confidential data or to the platform itself

5. Handling Requirements

Control	Public	Internal	Confidential	Restricted
Encryption in transit	Required	Required	Required	Required
Encryption at rest	Not required	Not required	Required	Required (AES-256)
Access control	Open	Authenticated	Need-to-know	Named individuals only
Logging	Not required	Basic	Full audit trail	Full audit trail
Sharing externally	Permitted	With discretion	Only with authorisation and appropriate agreements	Prohibited without executive approval
Retention	As needed	As needed	Per retention schedule	Per retention schedule, minimum necessary

5.1 How the platform meets these requirements

Requirement	How it is met
Encryption in transit	All web traffic uses HTTPS with TLS 1.2 or higher, and browsers are told to use HTTPS only. Connections to the database and cache require TLS
Encryption at rest	The database and its backups, the cache and file storage are encrypted at rest. Restricted values, such as integration credentials, connection secrets, webhook secrets and Direct Debit bank details, are additionally encrypted in the application with AES-256-GCM
Access control	Customer users have owner, manager or user roles within their own organisation, and two-factor authentication is enforced by default for new organisations. Platform secrets are held in AWS Secrets Manager and the application's encrypted credentials
Logging	Significant user and administrator actions are recorded in an audit log whose entries cannot be altered once written, including when a Subcontext administrator acts on a customer's behalf
Retention	Automatic retention periods are set out in the Data Retention & Deletion Policy

5.2 Rules for staff

- **Public:** may be published or shared freely once approved for publication
- **Internal:** kept within Subcontext's own systems and accounts; not posted publicly
- **Confidential:** accessed only through the platform or approved systems, only when needed for a task; never copied to personal devices, personal accounts or unapproved tools; never pasted into AI tools or services that are not approved sub-processors; exports are deleted once their purpose is served
- **Restricted:** never stored in source code, tickets, chat messages, email or documents; held only in AWS Secrets Manager or the application's encrypted credentials; shared only with the named individuals who need it; rotated immediately on any suspected exposure, in line with the Encryption & Key Management Policy

6. Customer Data

All customer data processed through the platform is classified as **Confidential** or higher. This includes:

- Contact personal data (names, emails, phone numbers)
- Conversation content
- Agent configurations and knowledge bases
- Integration credentials (classified as **Restricted**)
- Payment transaction data

Customer data also includes, and is treated as Confidential or higher:

- Call audio and voice recordings
- Insurance applications, quotes, policies and claims
- Health information collected for an insurance application, which is special category data under the UK GDPR and is collected only after explicit consent is recorded
- Direct Debit bank details, which are additionally encrypted in the application

Card details are never stored by Subcontext: they are handled by Stripe.

Customers decide what personal data they put into the platform and remain controllers of it. Subcontext applies this policy to all of it regardless of how the customer itself classifies it.

7. Classifying Data

7.1 When classification happens

- Data classification is determined at the point of creation or collection
- Each new feature, data store, integration or export is classified as part of its design, and the classification informs which controls are built in
- Classification is reviewed when data is combined, aggregated or moved to a new purpose, since combined data can be more sensitive than its parts

7.2 Worked examples

Data	Classification	Reason
A published policy on the trust centre	Public	Intended for public disclosure
A draft of the same policy before approval	Internal	Not yet for publication, not sensitive
An aggregated, anonymised usage chart with no customer named	Internal	No personal or customer-identifying data
A lead's name, phone number and conversation transcript	Confidential	Customer personal data
An export of a customer's leads as CSV	Confidential	Contains customer personal data, wherever it is stored
A customer's integration API key for its policy administration system	Restricted	Would give access to the customer's own systems
The database password or the application master key	Restricted	Would give access to all platform data

8. Roles and Responsibilities

- All employees are responsible for handling data in accordance with its classification
- **Directors:** approve this policy and any exception to it, and give the executive approval required before Restricted data is shared externally
- **Security Officer:** a member of the founding team who owns the security programme, maintains this policy, advises on classification questions and checks compliance
- **Data owners:** decide the classification of the data they are responsible for and make sure the right controls are applied
- **Staff:** handle data according to its classification, and report any mishandling or suspected exposure straight away under the Incident Response Plan
- **Customers:** as controllers, decide what data they place on the platform and who in their organisation can access it

When in doubt, apply the higher classification level.

9. Exceptions

Any exception to this policy, for example sharing Confidential data with a party not covered by an agreement, must be requested in writing to the Security Officer, setting out the data, the reason, the period and any compensating controls. Exceptions are approved by a director, recorded, time-limited and reviewed before they expire. Sharing Restricted data externally always requires executive approval.

10. Compliance

- The Security Officer checks compliance with this policy at least annually, including a review of where Confidential and Restricted data is stored and who can access it
- New features are checked against the handling requirements before release, as part of the Secure Development Policy
- Mishandling of data is treated as a security incident under the Incident Response Plan, and may lead to disciplinary action under the Staff Security Policy

11. Related Documents

- Information Security Policy
- Access Control Policy
- Encryption & Key Management Policy
- Data Retention & Deletion Policy
- Logging & Monitoring Policy
- Secure Development Policy
- Staff Security Policy
- Incident Response Plan
- Sub-Processor List

12. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and when the platform, its data or the law changes significantly
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.