ETS Connect UK User Rules of Engagement

16 June 2026
Version 1.1

Contents

CTP User Rules of Engagement

1. Document control

This document defines the Rules of Engagement (“RoE”) applicable to all users subscribing to data from the UK Bond Consolidated Tape (“CTP”).

This is a controlled document and subject to formal versioning. Updates may be issued periodically to reflect regulatory change, operational experience, or enhancements to the CTP service.

Normative language:
• MUST – mandatory requirement
• SHOULD – strong recommendationvs• MAY – optional capability

In the event of conflict, contractual and regulatory obligations take precedence.

1.1. Version History

Version	Date	Description
0.1	03/03/2026	Initial draft
1.0	30/03/2026	Approved Final version 1.0
1.1	08/06/2026	Realtime and Historical endpoints added.

2. Purpose and regulatory context

The purpose of this Rules of Engagement (“RoE”) is to define the technical and operational expectations applicable to Users accessing the UK Bond Consolidated Tape (“CT”).

This RoE establishes behavioural and system-level requirements to:

- preserve platform integrity and stability;
- ensure consistent and equitable access to CT data;
- promote orderly interaction with CTP interfaces;
- support compliance with applicable regulatory obligations.

This document governs technical access and usage behaviour and does not amend or replace the applicable Licence Agreement.

3. Scope and Applicability

These Rules apply to all Users authorised to access the CT, including:

- direct licensees of the CTP;
- Users accessing the CT via redistribution arrangements;
- all licence categories, unless otherwise specified.

This RoE applies to all supported CT delivery interfaces, including:

- FIX Market Data streaming;
- Real-Time CSV access via REST API;
- Historical data access via REST API.

These Rules apply to production environments and any environment designated by the CTP for operational data access.

Users are responsible for ensuring that their internal systems, downstream integrations, and third-party service providers adhere to these Rules.

4. General Principles of Access

Access to the CT is governed by the following principles:

4.1. Non-Discriminatory Treatment

The CTP operates the CT in a consistent and non-discriminatory manner within each licence category.

Technical controls, rate management, replay boundaries, and enforcement measures shall be applied proportionately and consistently to comparable Users.

4.2. Platform Integrity and Stability

Users must interact with CTP interfaces in a manner that preserves service stability and does not introduce avoidable operational risk.

The CTP applies operational controls designed to preserve platform integrity, ensure equitable access, and maintain service stability across all supported interfaces.

4.3. Proportionate Operational Controls

Where user behaviour materially impacts infrastructure load, sequencing integrity, or service performance, the CTP may implement proportionate technical controls, including rate management or session controls.

Such measures are intended to protect platform stability and are not designed to restrict legitimate use.

4.4. UTC Time Standard

All operational boundaries, including replay windows and publication timestamps, are aligned to Coordinated Universal Time (UTC). Users must ensure appropriate handling of UTC-based sequencing and day boundaries.

4.5. Consistency Across Access Channels

These Rules apply equally to Users accessing the CT directly or via redistribution. Redistribution arrangements do not alter technical or operational obligations.

5. Supported Interfaces

The UK Bond Consolidated Tape is made available to authorised Users through the following delivery mechanisms:

Interface	Delivery Model	Intended Use
FIX Market Data	Persistent streaming session	Real-time, low-latency consumption
Real-Time CSV (REST API)	Polling / retrieval-based	Near real-time structured
Historical File Collection (REST API)	File download	End-of-day and backfill use

Each interface is governed by this Rules of Engagement. Behavioural and operational expectations are consistent across interfaces, unless otherwise specified.

PART A – FIX Market Data Interface

6. Environments and access

This section defines the environments, access controls, and onboarding requirements applicable to Users consuming UK Bond Consolidated Tape data via FIX.

Separate environments are provided for pre-production validation and live operation. Users MUST ensure configuration parity between environments.

Production environments MUST NOT be used for testing or development activities.

Separate environments are provided for certification and production.
Production must not be used for testing. Configuration parity between environments is mandatory.

6.1. Available Environments

The CTP provides the following FIX environments:

Environment	Intended Function
UAT (User Acceptance Testing)	Pre-production integration, functional validation, and client readiness testing. Users SHOULD validate FIX session behaviour, message handling, recovery scenarios, and duplicate processing logic in this environment.
PROD (Production)	Live operational FIX connectivity and receipt of consolidated tape data. Access is restricted to authorised Users that have completed onboarding and received explicit production approval.

Each environment is logically isolated and operates with independent connectivity endpoints, credentials, and certificates.

6.2. User Onboarding and Authorisation

Prior to accessing any FIX environment, Users MUST complete the CTP onboarding process, including:

- execution of applicable User agreements;
- registration of operational and technical contacts;
- allocation of FIX identifiers (SenderCompID / TargetCompID);
- IP address allowlisting;
- issuance and installation of mTLS certificates;
- confirmation of selected regions (single-region or dual-region connectivity).

Access to Production is granted only after successful completion of onboarding and explicit CTP authorisation.

Unlike Contributors, Users are not subject to formal FIX certification; however, Users remain fully responsible for validating their own readiness prior to Production access.

6.3. Identity and Credentials

Each User is issued with unique FIX session identifiers and authentication credentials.

Users MUST:

- use credentials strictly as allocated;
- prevent sharing of credentials across systems or legal entities;
- protect credentials against unauthorised access;
- immediately notify the CTP of any suspected compromise.

CTP reserves the right to suspend or revoke access where credential integrity cannot be assured.

6.4. Environment Isolation

Trust anchors, certificate authorities, and certificate chains are segregated between UAT and Production.

Certificates issued for one environment MUST NOT be reused in another.

Users MUST maintain separate configurations per environment.

6.5. Regional Access

The UK Bond CTP operates an active-active regional architecture.

Users may elect to connect to:

- a single region; or
- multiple regions for resilience.

Where Users connect to multiple regions, they MUST comply with the Technical Duplicate handling requirements defined in Section 10.

The CTP does not guarantee identical publication timestamps or delivery order across regions.

6.6. Acceptable Use

Users MUST:

- consume CT data only for authorised purposes;
- operate FIX sessions in accordance with this RoE;

- avoid behaviour that could degrade platform stability (including aggressive reconnect loops, uncontrolled replay attempts, or excessive session churn).

Production endpoints MUST NOT be used for load testing, benchmarking, or synthetic traffic generation.

Non-compliant behaviour may result in throttling, suspension, or revocation of access.

7. FIX Connectivity and transport requirements

This section defines the mandatory technical and security requirements governing FIX connectivity between Users and the CTP FIX Market Data Gateway.

All Users consuming CT data via FIX MUST comply with the requirements set out below.

7.1. Transport Protocol and Session Establishment

FIX market data sessions MUST:

- operate over persistent TCP connections;
- use FIX tag=value encoding as defined in the UK Bond CT FIX specification
- CT-with-FIX-Protocol-1.0.1-UK-B...
- establish a valid FIX Logon (35=A) exchange prior to receiving application-level messages.

Users MUST NOT transmit application-level messages (other than Logon, Logout, TestRequest, Heartbeat, ResendRequest, or SequenceReset) prior to successful session establishment.

Each FIX session is uniquely identified by allocated SenderCompID and TargetCompID values.

7.2. Mutual TLS (mTLS) Security

All FIX connectivity MUST be secured using mutual Transport Layer Security (mTLS).

Requirements:

- TLS version 1.2 or higher;
- X.509 certificate presentation by both parties;
- successful TLS handshake prior to FIX session establishment.

Sessions MUST NOT be established where certificate validation fails.

Users are responsible for secure storage and protection of private keys.

7.3. Certificate Lifecycle Management

Client certificates:

- are issued by the CTP or a CA operating under its control;
- have a maximum validity period of 12 months;
- must be renewed prior to expiry.

Users MUST initiate certificate renewal no later than thirty (30) calendar days prior to expiry.

Expired, revoked, or compromised certificates may result in immediate connection refusal.

Any suspected compromise MUST be reported to the CTP immediately.

7.4. Connection Management and Reconnect Behaviour

Users MUST implement controlled reconnect behaviour consistent with platform stability requirements.

Reconnect attempts MUST:

- apply exponential backoff with randomised jitter;
- begin with a delay of no less than five (5) seconds;
- double on each subsequent failure;
- cap at a maximum retry interval of three hundred (300) seconds.

The following behaviours are prohibited:

- fixed-interval rapid reconnect loops;
- parallel reconnect attempts for the same FIX session;
- reconnect storms during regional or network instability.

Backoff behaviour MUST apply regardless of disconnect cause, including:

- network failure;
- receipt of Logout (35=5);
- Logon rejection;
- TLS handshake failure.

Repeated non-compliant reconnect behaviour may result in throttling or temporary suspension.

7.5. Session Concurrency and Capacity

Users MUST NOT establish more FIX sessions than explicitly authorised.

Session multiplexing, session splitting, or dynamic scaling of FIX sessions is not permitted unless agreed in writing by the CTP.

Users are responsible for ensuring their systems can sustain authorised message volumes without introducing instability.

7.6. Regional Connectivity

Users connecting to multiple regions MUST:

- establish independent FIX sessions per region;
- treat each region as logically independent for connectivity purposes;
- ensure client systems can tolerate asynchronous delivery between regions.

The CTP does not guarantee identical message timing or ordering across regions.

Dual-region Users MUST comply with the Technical Duplicate requirements set out in Section 10.

7.7. Monitoring and Enforcement

The CTP may monitor:

- TLS handshake behaviour;
- certificate usage;
- session establishment patterns;
- reconnect frequency;
- session stability metrics.

Where non-compliant behaviour is observed, the CTP may:

- issue warnings;
- throttle sessions;
- administratively Logout sessions;
- temporarily suspend connectivity.

Persistent or material breaches may result in access revocation.

8. FIX session rules

This section defines the mandatory FIX session-layer behaviours applicable to all Users consuming UK Bond Consolidated Tape data.

Users MUST operate FIX sessions in full compliance with FIX Trading Community session standards and this Rules of Engagement.

8.1. Session Lifecycle

Each FIX session MUST follow the standard lifecycle:

- Logon (35=A)
- steady-state message exchange
- Logout (35=5)

Users MUST successfully complete the Logon exchange before processing application-level messages.

Where practicable, sessions SHOULD be terminated gracefully using Logout.

Forced disconnects MUST be used where session integrity cannot be maintained.

8.2. Heartbeats and Liveness

Users MUST:

- honour the negotiated HeartBtInt;
- send Heartbeat (35=0) messages when no application messages are received within the heartbeat interval;
- respond to TestRequest (35=1) with an immediate Heartbeat containing the corresponding TestReqID.

Failure to maintain heartbeat discipline may result in administrative Logout.

8.3. Message Sequencing

Users MUST:

- process inbound messages strictly in ascending MsgSeqNum order;
- detect sequence gaps;
- issue ResendRequest (35=2) where gaps are identified;
- correctly process replayed messages and SequenceReset (35=4) Gap Fill messages.

Application messages MUST NOT be processed out of sequence.

8.4. Recovery and Replay

Users MUST support standard FIX recovery mechanisms, including:

- ResendRequest handling;

- Gap Fill processing;
- clean session restart following disconnect.

Replay support is limited to the current UTC business day.

Users MUST NOT attempt bulk recovery by repeatedly resetting sessions.

Users MUST ensure replayed messages are handled idempotently.

8.5. Sequence Reset Controls

Users MUST NOT issue unsolicited SequenceReset messages.

Sequence resets may only occur:

- as part of standard Gap Fill processing; or
- when explicitly coordinated with the CTP.

Unauthorised sequence resets may result in session termination.

8.6. Idempotent Processing

Users MUST implement idempotent processing of inbound messages.

Repeated delivery of the same application message may occur during:

- recovery;
- replay;
- reconnect scenarios.

Users MUST ensure such messages do not corrupt downstream state or cause double-counting.

8.7. Behaviour During Degraded Conditions

During CTP incidents, degraded modes, or recovery events, Users MUST:

- follow instructions issued by the CTP;
- avoid uncontrolled reconnect or replay behaviour;
- refrain from actions that could exacerbate instability.

CTP operational instructions take precedence over standard session behaviour.

9. Sequence numbers, recovery and replay

This section defines the requirements for message sequencing, session recovery, and replay applicable to Users consuming UK Bond Consolidated Tape data via FIX.

Users MUST support standard FIX recovery mechanisms and ensure downstream systems can tolerate message replay and re-delivery without data corruption.

9.1. Message Sequencing

Users MUST:

- process inbound FIX messages strictly in ascending MsgSeqNum (Tag 34) order;
- detect sequence gaps;
- issue ResendRequest (35=2) when gaps are identified;
- correctly process replayed messages and SequenceReset (35=4) Gap Fill messages.

Application-level messages MUST NOT be processed out of sequence.

Users MUST preserve sequencing state across disconnects and reconnects.

Failure to correctly manage sequencing may result in inconsistent downstream state.

9.2. Standard FIX Recovery

Users MUST support standard FIX recovery behaviour, including:

- gap detection;
- ResendRequest handling;
- replay processing;
- Gap Fill interpretation.

Replayed messages MUST be handled idempotently.

Users MUST NOT assume that a message is unique simply because it is received only once during steady-state operation.

Repeated delivery of the same message may occur during recovery scenarios.

9.3. Replay Scope and Limitations

The CTP supports FIX replay for messages published during the current UTC business day only.

Replay is provided exclusively via standard FIX session recovery mechanisms.

Users MUST NOT attempt to obtain historical data by repeatedly resetting FIX sessions or inducing reconnect cycles.

Historical data outside the current UTC day is made available via the Historical File REST interface and is not supported via FIX replay.

9.4. Clean Restart Behaviour

Following client-side restart or network interruption, Users MUST:

- re-establish FIX sessions in accordance with Section 8;
- correctly recover message sequence state;
- ensure replayed messages are processed safely and idempotently;
- avoid uncontrolled reconnect or replay loops.

Users are responsible for ensuring downstream systems do not double-count transactions as a result of recovery activity.

9.5. Replay and Duplicate Handling

Users MUST assume that replayed messages may include:

- previously processed application messages;
- partial state re-delivery;
- repeated transmission of identical payloads.

Users MUST implement deterministic handling to prevent corruption of internal state.

Additional requirements for Users connecting to multiple regions are defined in Section 10 (Dual-Region Connectivity and Technical Duplicates).

9.6. Prohibited Behaviour

Users MUST NOT:

- repeatedly reset FIX sessions to force replay;
- issue unauthorised SequenceReset messages;
- attempt bulk recovery through reconnect loops;
- rely on publication timestamps to determine message uniqueness.

Such behaviour may result in throttling, administrative Logout, or suspension of access.

10. Dual-Region Connectivity and Technical Duplicates

The UK Bond CTP operates an active-active regional architecture. Users may elect to connect to one or more CTP regions for resilience purposes.

Where Users consume data from multiple regions, they may receive duplicate messages representing the same economic transaction (“Technical Duplicates”).

Technical Duplicates arise from independent regional publication paths and do not represent distinct economic events.

10.1. Definition of Technical Duplicate

A Technical Duplicate occurs where all economic and regulatory attributes of a transaction are identical, and any differences are limited solely to:

- CTP reception timestamp metadata (i.e. TrdRegTimestamp where TrdRegTimestampType = 2 and `TrdRegTimestampOrigin = P);
- CTP publication timestamp metadata (i.e. TrdRegTimestamp where TrdRegTimestampType = 11 and `TrdRegTimestampOrigin = P);
- Contributor-supplied non-economic timestamps provided exclusively for latency measurement or operational monitoring purposes.

Such fields are observational only and MUST NOT be used to determine transaction uniqueness.

Messages that differ in lifecycle state (New / Amend / Cancel) or economic content are not Technical Duplicates and MUST be processed independently.

10.2. Technical Duplicate Identification Attributes

When connecting to multiple regions, Users SHOULD identify Technical Duplicates at the individual trade (MDEntry) level using the following attributes.

A message entry may be treated as a Technical Duplicate only where all of the following are identical:

Transaction Identity

- RegulatoryTradeID and/or RegulatoryTradeIDGrp

Instrument Identification

- SecurityID
- SecurityIDSource
- Symbol (where present)

Lifecycle State

- MDUpdateAction
- MDEntryType

Economic Terms (where present)

- MDEntryPx
- PriceType
- MDEntrySize

- Currency

Venue and Party Information

- LastMkt
- Party identifiers and roles (where supplied)

Transparency and Regulatory Flags (as applicable)

Including, but not limited to:

- trade classification fields
- deferral indicators
- publication type / reason
- regulatory report type
- data quality indicators

These materially affect regulatory meaning and MUST participate in duplicate identity.

Duplicate detection MUST be performed per MDEntry. Users MUST NOT assume a one-to-one relationship between FIX messages and economic transactions.

10.3. Explicit Exclusions

Users MUST exclude the following from duplicate identity:

- CTP reception timestamp (TrdRegTimestampType = 2, Origin = P);
- CTP publication timestamp (TrdRegTimestampType = 11, Origin = P);
- contributor-supplied non-economic observability or latency timestamps.

These fields may legitimately differ between regions and MUST NOT be used to infer uniqueness.

10.4. User Responsibilities

Users connecting to multiple regions MUST:

- implement deterministic duplicate detection logic based on economic attributes;
- de-duplicate Technical Duplicates prior to downstream processing;
- ensure idempotent handling of replay and recovery scenarios;
- prevent double-counting in analytics, valuation, or regulatory workflows;
- tolerate asynchronous delivery and differing publication timestamps between regions.

The CTP does not guarantee identical message timing or ordering across regions.

10.5. Interaction with Recovery and Replay

Technical Duplicates may occur during:

- normal dual-region operation;
- FIX recovery and replay;
- client restart scenarios.

Users MUST ensure their duplicate handling logic operates consistently across steady-state, recovery, and replay conditions.

Publication timestamps MUST NOT be relied upon to distinguish unique economic events.

11. FIX Message Consumption Rules

This section defines the requirements for consuming and processing UK Bond Consolidated Tape messages delivered via FIX.

Users MUST comply with the message semantics defined in the UK Bond CT FIX specification and this Rules of Engagement.

11.1. Supported Message Types

Users will receive the following FIX message types:

- MarketDataRequest (35=V) — subscribe to post-trade CT updates
- MarketDataIncrementalRefresh (35=X) — delivery of post-trade CT updates
- Reject (35=3) — session level rejects

Users MUST support all mandatory fields and repeating groups defined for these message types.

11.2. Atomic Processing Unit

Each MarketDataIncrementalRefresh (35=X) message published by CTP contains a single trade entry (one MDEntry instance only).

Accordingly, the FIX message itself represents the atomic unit of processing.

Users MUST treat each received 35=X message as a discrete, independently processable trade event.

Users MUST NOT infer message-level batching semantics or assume that multiple economic transactions are contained within a single FIX message.

Duplicate detection, lifecycle handling (e.g., NEW, CANCEL, CORRECT), sequencing, and all downstream processing logic MUST operate at the individual message level.

Where lifecycle linkage is required (e.g., cancellation or correction referencing a prior trade), Users MUST rely on the appropriate trade identifiers and reference fields provided in the message, rather than positional or batching assumptions.

11.3. Lifecycle Handling

Users MUST correctly process the full lifecycle of each transaction, including:

- New (MDUpdateAction = 0)
- Amend (MDUpdateAction = 1)
- Cancel (MDUpdateAction = 2)

Lifecycle events MUST be applied in sequence and reflected accurately in downstream systems.

Users MUST NOT collapse or suppress Amend or Cancel events through duplicate handling logic.

11.4. State Management

Users are responsible for maintaining accurate internal state for each transaction, including:

- applying Amend events to the correct original record;
- removing or invalidating records upon Cancel;
- ensuring consistency across recovery and replay scenarios.

Users MUST retain sufficient identifiers to correlate lifecycle events.

11.5. Data Quality Notifications

Where MarketDataAck (35=EQ) messages are provided, Users SHOULD consume these for operational awareness.

Data quality flags or warnings do not alter the lifecycle semantics of transactions and MUST NOT be interpreted as corrections or cancellations unless explicitly indicated via MDUpdateAction.

11.6. Ordering and Dependency

Users MUST process MDEntries in the order received within a FIX session, subject to sequencing guarantees defined in Sections 8 and 9.

Users MUST NOT apply later lifecycle events before earlier ones for the same transaction.

Out-of-order handling caused by client-side buffering or parallelism is the User's responsibility.

11.7. Prohibited Behaviour

Users MUST NOT:

- infer economic meaning from FIX envelope ordering across regions;
- treat FIX messages as transactional containers;
- suppress Amend or Cancel events as duplicates;
- rely on publication timestamps to determine lifecycle order.

Such behaviour may result in inconsistent downstream representations of the consolidated tape.

12. Data Handling Expectations (FIX)

This section defines the responsibilities of Users with respect to the handling, storage, interpretation, and downstream use of UK Bond Consolidated Tape data received via FIX.

The CTP provides consolidated output based on contributor submissions and applies validation and enrichment in support of publication. Users remain fully responsible for their downstream processing and use of CT data.

12.1. Economic vs Observational Attributes

CT messages contain a combination of:

- economic and regulatory attributes (e.g. price, size, identifiers, transparency flags); and
- observational or technical metadata (e.g. publication timestamps, contributor performance timestamps).

Users MUST distinguish between these categories.

Observational attributes MUST NOT be used to:

- infer economic uniqueness;
- drive lifecycle logic;
- override contributor execution timestamps;
- replace regulatory trade identifiers.

12.2. Downstream Processing Responsibility

Users are responsible for:

- maintaining accurate internal representations of transactions;
- applying lifecycle events correctly;
- ensuring deterministic duplicate handling;
- preventing double-counting during replay or recovery;

- preserving auditability of downstream state.

The CTP does not guarantee fitness for any specific User application, analytics model, or valuation methodology.

12.3. Redistribution and Derived Use

Where Users redistribute CT data or create derived datasets, they MUST:

- preserve the economic integrity of the original records;
- ensure Amend and Cancel events are propagated appropriately;
- avoid selective suppression of regulatory attributes;
- comply with all contractual redistribution requirements.

Derived datasets MUST NOT misrepresent transaction state or regulatory flags.

12.4. Interpretation of Data Quality Indicators

Data quality indicators or warnings provided by the CTP are intended for operational awareness.

Such indicators:

- do not alter transaction lifecycle;
- do not invalidate published trades unless explicitly cancelled via MDUpdateAction;
- MUST NOT be treated as corrections.

Users remain responsible for determining how such indicators are reflected in downstream systems.

12.5. Data Retention and Auditability

Users MUST retain sufficient data and logs to:

- reconcile FIX consumption;
- demonstrate correct lifecycle handling;
- support incident investigation;
- respond to reasonable supervisory or CTP requests.

Retention policies must align with applicable regulatory and contractual requirements.

13. Rejects, errors, notifications and remediation

This section defines the handling of session-level and application-level errors applicable to Users consuming UK Bond Consolidated Tape data via FIX.

Users MUST implement appropriate controls to detect, investigate, and remediate errors affecting FIX session integrity or message processing.

13.1. Session-Level Rejects

Session-level Reject messages (35=3) indicate protocol or structural validation failures, including but not limited to:

- invalid or missing mandatory tags;
- invalid tag formats;
- unsupported MsgType values;
- sequence violations;
- incorrect tag ordering.

Upon receipt of a session-level Reject, Users MUST:

- investigate the root cause;
- correct protocol defects prior to resuming normal processing;
- avoid repeated transmission of malformed messages.

Persistent session-level errors may result in administrative Logout or suspension of connectivity.

13.2. Administrative Logout

The CTP may issue Logout (35=5) messages where:

- protocol violations occur;
- sequencing cannot be maintained;
- authentication fails;
- unacceptable reconnect behaviour is detected;
- security issues are identified.

Upon receipt of Logout, Users MUST:

- cease message transmission immediately;
- close the session cleanly;
- apply reconnect backoff in accordance with Section 7.

13.3. MarketDataAck (Application-Level Notifications)

Where enabled, MarketDataAck (35=EQ) messages may be received for operational transparency.

Such acknowledgements may indicate:

- acceptance;
- acceptance with data quality warning;

- rejection of specific message content (where applicable).

Users SHOULD monitor these acknowledgements for operational awareness.

MarketDataAck messages do not alter lifecycle semantics and MUST NOT be treated as economic updates unless explicitly conveyed via MDUpdateAction.

13.4. Error Investigation and Remediation

Users MUST:

- implement monitoring sufficient to detect session instability or error conditions;
- investigate persistent rejects or abnormal behaviour;
- remediate defects in a timely manner;
- notify the CTP where errors materially impact data consumption.

Repeated failure to remediate defects may result in enforcement measures under Section 19.

13.5. Evidence and Audit

Users MUST retain sufficient logs to:

- reconstruct FIX sessions;
- demonstrate sequencing compliance;
- evidence recovery behaviour;
- support post-incident analysis.

Evidence may be requested by the CTP during operational or supervisory review.

14. Operational Resilience (FIX)

Users consuming UK Bond Consolidated Tape data via FIX are expected to operate their consumption services with a level of resilience proportionate to their market role and downstream reliance on CT data.

Users remain responsible for ensuring that their internal systems can tolerate network disruption, replay, duplicate delivery, and regional failover without corrupting downstream state.

14.1. Restart and Recovery Capability

Users MUST maintain the ability to:

- tolerate transient infrastructure failures;
- recover cleanly from FIX session disconnects;
- correctly process replayed messages;

- resume data consumption without double-counting or data loss.

Client restart procedures MUST be tested periodically.

14.2. Behaviour During CTP Incidents

During CTP incidents, degraded modes, or recovery events, Users MUST:

follow instructions issued by the CTP;

- avoid uncontrolled reconnect attempts;
- refrain from inducing replay through repeated session resets;
- avoid behaviour that could exacerbate instability.

CTP-issued operational instructions take precedence over standard session behaviour.

14.3. Dual-Region Resilience

Users connecting to multiple regions MUST ensure their systems can:

- tolerate asynchronous message delivery;
- tolerate differing publication timestamps;
- handle Technical Duplicates deterministically;
- operate correctly if one region becomes temporarily unavailable.

Regional failover MUST NOT introduce downstream duplication or lifecycle corruption.

The CTP does not guarantee identical timing, ordering, or latency characteristics across regions.

14.4. Capacity and Performance Management

Users are responsible for ensuring that their systems:

- can process authorised message volumes;
- can tolerate replay bursts during recovery;
- do not introduce back-pressure that causes session instability.

Users MUST NOT use production FIX sessions for stress testing or benchmarking.

14.5. Monitoring and Alerting

Users SHOULD implement monitoring for:

- session connectivity status;
- sequencing gaps;
- replay frequency;

- duplicate detection activity;
- abnormal disconnect patterns.

Monitoring controls MUST be sufficient to detect and remediate operational defects in a timely manner.

14.6. Resilience Testing

Users SHOULD periodically validate their ability to:

- restart client systems;
- recover FIX sessions;
- correctly process replay;
- correctly handle Technical Duplicates;
- tolerate regional failover scenarios.

Where requested, Users may be invited to participate in coordinated readiness or resilience exercises.

15. Time Synchronisation

Accurate and consistent time synchronisation is important to the correct interpretation, reconciliation, and monitoring of UK Bond Consolidated Tape data.

Users are responsible for ensuring that their internal systems maintain appropriate time discipline when consuming CT data via FIX.

15.1. UTC Reference Standard

All timestamps published by the CTP are expressed in UTC.

Users MUST:

- interpret all CT timestamps as UTC;
- align internal processing systems to a recognised authoritative UTC time source (e.g. NTP or equivalent);
- ensure consistent treatment of time zones across downstream systems.

Failure to correctly interpret UTC timestamps may result in incorrect replay, reconciliation, or lifecycle sequencing.

15.2. Clock Synchronisation

Users SHOULD:

- synchronise system clocks using a reliable time synchronisation mechanism;
- monitor clock drift on an ongoing basis;
- ensure application servers involved in FIX consumption remain within acceptable tolerance of UTC.

Unsynchronised local clocks may result in incorrect ordering, reconciliation gaps, or inaccurate latency monitoring.

15.3. Interpretation of CT Timestamps

CT messages may contain:

- contributor execution timestamps;
- regulatory reporting timestamps;
- CTP publication timestamps.

Users MUST:

- distinguish between economic execution time and CTP publication time;
- avoid using publication timestamps to infer economic sequence;
- avoid using observational timestamps to determine transaction uniqueness (see Section 10).

Publication timestamps reflect the time of regional publication and may differ between regions.

15.4. Replay Boundary Considerations

FIX replay is limited to the current UTC business day.

Users MUST ensure that:

- replay logic respects UTC date boundaries;
- downstream systems correctly handle day transitions;
- restart and recovery procedures account for UTC rollover.

Incorrect handling of UTC boundaries may result in incomplete replay or duplication.

15.5. Monitoring and Audit

Users SHOULD retain sufficient time-based logging to:

- reconcile session restart times;
- measure replay windows;

evidence sequencing behaviour during incident investigation.

16. Change Management (FIX)

This section defines the obligations of Users to notify and manage changes that may affect the stability, integrity, or correct consumption of UK Bond Consolidated Tape data via FIX.

Users MUST operate appropriate internal change management controls for systems used to consume CT data.

16.1. Material Changes

Users MUST notify the CTP in advance of any material change that may reasonably impact:

- FIX session stability;
- sequencing, recovery, or replay behaviour;
- duplicate handling logic;
- regional connectivity;
- downstream interpretation of CT data.
- Material changes include, but are not limited to:
- FIX engine replacement or major version upgrade;
- changes to FIX session configuration (e.g. HeartBtInt, sequence handling);
- changes to SenderCompID / TargetCompID usage;
- changes to certificate handling or TLS configuration;
- introduction or removal of dual-region connectivity;
- changes to deduplication or lifecycle processing logic;
- significant changes to consumption volume or processing architecture.

16.2. Non-Material Changes

The following are generally considered non-material, provided behaviour is unchanged:

- minor software patches or bug fixes;
- infrastructure or operating system changes that do not alter FIX behaviour;
- internal monitoring or logging enhancements.

Where there is doubt, Users SHOULD notify the CTP.

16.3. Change Notification Expectations

For material changes, Users SHOULD:

- notify the CTP in advance where practicable;
- provide a high-level description of the change;
- identify any potential impact to FIX consumption or resilience;

- coordinate timing where changes may affect stability.

The CTP may request additional information or impose reasonable conditions to protect platform stability.

16.4. Post-Change Responsibility

Users remain responsible for ensuring that:

- FIX sessions operate correctly following change;
- sequencing and replay behaviour remains compliant;
- duplicate handling continues to function correctly;
- downstream systems remain consistent.

Where a change results in instability or non-compliant behaviour, the CTP may require remediation or suspend access until issues are resolved.

16.5. Emergency Changes

In the case of emergency changes required to remediate incidents or security issues:

- Users MUST notify the CTP as soon as reasonably practicable;
- retrospective details of the change MUST be provided upon request.

17. Monitoring, Evidence, and Audit (FIX)

Users consuming UK Bond Consolidated Tape data via FIX MUST maintain monitoring and record-keeping controls sufficient to support stable operation, incident investigation, and supervisory review.

17.1. Monitoring Expectations

Users SHOULD implement monitoring appropriate to their scale and usage, including:

- FIX session connectivity status;
- disconnect and reconnect frequency;
- sequencing gaps and replay activity;
- duplicate detection events;
- abnormal message volumes or processing delays.

Monitoring MUST be sufficient to detect material operational issues in a timely manner.

17.2. Log Retention

Users MUST retain sufficient logs to:

- reconstruct FIX session activity;
- demonstrate sequencing compliance;
- evidence replay handling;
- support investigation of duplicate or lifecycle anomalies.

Retention periods MUST comply with contractual and regulatory obligations.

17.3. Evidence Provision

Upon reasonable request, Users MUST be able to provide evidence relating to:

- FIX session behaviour;
- recovery and replay events;
- duplicate handling logic;
- incident timelines.

Evidence may be requested in connection with operational incidents, platform investigations, or supervisory review.

17.4. Internal Review

Users SHOULD periodically review their FIX consumption arrangements to confirm ongoing compliance with this Rules of Engagement, including:

- replay handling;
- dual-region behaviour (where applicable);
- lifecycle processing;
- resilience controls.

18. Incident Management and Escalation

This section defines the obligations of Users to notify and cooperate with the CTP in relation to incidents affecting the consumption of UK Bond Consolidated Tape data.

Users MUST maintain appropriate incident management processes to detect, respond to, and remediate issues impacting FIX connectivity or downstream data integrity.

18.1. Incident Notification

Users MUST promptly notify the CTP of any incident that materially impacts:

- FIX session stability;
- sequencing, recovery, or replay behaviour;
- duplicate handling;
- downstream representation of CT data;
- ability to consume CT data in a timely manner.
- Notification SHOULD include:
- a brief description of the issue;
- affected environments or regions;
- approximate start time;
- initial assessment of impact.

18.2. Cooperation and Resolution

During incident resolution, Users MUST:

- cooperate fully with CTP operational teams;
- provide relevant logs or evidence upon request;
- follow CTP instructions regarding reconnect timing, replay behaviour, or operational sequencing.
- CTP instructions issued during incidents take precedence over standard operating behaviour.

18.3. Post-Incident Review

Following material incidents, Users SHOULD participate in post-incident review activities where requested.

This may include:

- sharing root cause analysis;
- confirming remediation actions;
- validating recovery behaviour;
- demonstrating improvements to prevent recurrence.

18.4. User Responsibility

Users remain responsible for:

- restoring normal operation of their systems;
- ensuring downstream state integrity;
- preventing repeat incidents arising from unresolved defects.
- Repeated failure to remediate issues may result in enforcement measures under Section 19.

19. Enforcement

The CTP applies a graduated enforcement model to ensure stable, fair, and compliant access to UK Bond Consolidated Tape data.

Failure to comply with this Rules of Engagement may result in enforcement action.

19.1. Graduated Enforcement Model

Where non-compliant behaviour is identified, the CTP may apply one or more of the following measures:

- informal notification or warning;
- request for remediation within a defined timeframe;
- enhanced monitoring;
- temporary throttling of FIX sessions;
- administrative Logout;
- temporary suspension of connectivity;
- revocation of access.

Enforcement measures will be proportionate to the severity, persistence, and impact of the non-compliance.

19.2. Examples of Non-Compliance

Non-compliant behaviour includes, but is not limited to:

- repeated sequencing violations;
- uncontrolled reconnect or replay attempts;
- failure to implement duplicate handling when connected to multiple regions;
- misuse of publication timestamps to infer economic uniqueness;
- unauthorised session resets;
- use of production environments for testing or load generation;
- failure to remediate identified defects.

19.3. Urgent Protective Action

The CTP reserves the right to take immediate protective action, including temporary suspension, where necessary to:

- protect platform stability;
- prevent systemic disruption;
- address security risks;

- ensure market integrity.

Such action may be taken without prior notice where circumstances require.

19.4. Reinstatement

Where access is suspended, reinstatement may require:

- demonstration of remediation;
- validation of compliant behaviour;
- confirmation of operational readiness.

20. Confidentiality and Data Handling

This section defines the obligations of Users with respect to the confidentiality, protection, and permitted use of UK Bond Consolidated Tape data and CTP connectivity endpoints.

20.1. Confidentiality of Access Credentials and Endpoints

Users MUST protect all CTP-issued credentials, certificates, and endpoint details against unauthorised access or disclosure.

Users MUST NOT:

- share credentials across legal entities, systems, or third parties;
- disclose endpoint details except where strictly necessary for authorised integration or support purposes.

Any suspected compromise MUST be reported to the CTP without undue delay.

20.2. Permitted Use of CT Data

Users MUST use CT data solely in accordance with:

- their contractual permissions;
- applicable regulatory requirements;
- this Rules of Engagement.

CT data MUST NOT be used in a manner that misrepresents transaction state, regulatory flags, or market transparency outcomes.

20.3. Data Protection and Security

Users MUST implement reasonable technical and organisational measures to protect CT data against:

- unauthorised access;
- unauthorised modification;
- loss or corruption.

Security controls should be proportionate to the sensitivity and downstream reliance on the data.

20.4. Redistribution and Third-Party Access

Where Users redistribute CT data or make it available to third parties, they remain responsible for:

- ensuring redistribution is contractually permitted;
- preserving the integrity of economic and regulatory attributes;
- ensuring Amend and Cancel events are propagated appropriately;
- preventing misleading or incomplete representations of the consolidated tape.

20.5. Retention and Disposal

Users MUST retain and dispose of CT data in accordance with:

- contractual requirements;
- applicable regulatory obligations;
- internal data governance policies.

Data disposal MUST be performed securely.

PART B - Real-Time CSV via REST API

21. Real-Time CSV Interface Overview

The Real-Time CSV interface provides structured post-trade CT data via a REST-based retrieval mechanism.

Unlike FIX, this interface operates on a polling and file retrieval model rather than a persistent session.

- Users remain responsible for:
- correct polling behaviour;
- duplicate handling;

- lifecycle integrity;
- resilience and recovery.

21.1. Realtime CSV Access and Authentication

Users MUST:

- authenticate using issued credentials or API tokens;
- protect credentials from unauthorised disclosure;
- use authorised IP ranges where applicable.
- Authentication methods and endpoint details are environment-specific.

21.2. Endpoints and Environment Configuration

The Real-Time CSV interface is accessed via REST API endpoints specific to each environment. The Real-Time CSV endpoint shares a common API host with the Historical interface, with access differentiated by resource path. The following endpoint is provided:

Environment	Endpoint	IP Addresses	Path
UAT	https://data-api-uat.ets-connect.co.uk		/v1/bonds/realtime/minute/window?start=<YYYY-MM-DDTHH:mm:00Z>
Production	https://data-api.ets-connect.co.uk	167.254.164.46 167.254.165.46	/v1/bonds/realtime/minute/window?start=<YYYY-MM-DDTHH:mm:00Z>

Users MUST:

- ensure that the correct endpoint is used for the target environment;

- avoid use of Production endpoints for testing or validation;

- maintain separate configurations for UAT and Production environments.

All endpoints:

- require Auth0 authentication as defined in Section 22;

- operate over HTTPS (TLS 1.2 or higher).

21.3. Authentication and Authorization (Auth0)

Users MUST authenticate all REST API requests using Auth0-issued credentials.

Supported Authentication Method:

- OAuth 2.0 Client Credentials Flow
- Using:
    - client_id
    - client_secret
    - organization

Token Acquisition:

- Users MUST obtain an access token from the Auth0 token endpoint prior to invoking any REST API
- The access token MUST be included in all API requests

Token Request Example:

```
POST /oauth/token HTTP/1.1
Host: <tenant>.eu.auth0.com
Content-Type: application/json
{
  "client_id": "<your client ID>",
  "client_secret": "<your client secret>",
  "audience": "<audience>",
  "grant_type": "client_credentials",
  "organization": "<your org_id>"
}
```

Request Requirements:

- API requests MUST include a valid bearer token:

```
Authorization: Bearer <access_token>
```

Operational Expectations:

- Clients MUST:
    - manage token lifecycle (including expiry and refresh)
    - avoid requesting tokens excessively
    - securely store client credentials

Security Requirements:

- client_id and client_secret MUST be treated as confidential credentials
- Credentials MUST NOT be embedded in client-side or publicly accessible applications
- Any suspected credential compromise MUST be reported immediately

Failure Behaviour:

- Requests with invalid or expired tokens will be rejected
- Repeated unauthorised requests may result in rate limiting or access suspension

Applicability:

- This authentication model applies to:
    - Real-Time CSV REST API
    - Historical Data REST API

22. Real-Time CSV Delivery Model

The Real-Time CSV interface:

- provides incremental CT updates;
- reflects lifecycle events (New / Amend / Cancel);
- may include publication timestamps;
- operates in UTC.

Users MUST NOT assume one file equals one transaction.

Files may contain multiple records.

23. Polling and Rate Discipline

Users MUST:

- implement reasonable polling intervals;
- apply exponential backoff when errors occur;
- avoid excessive or burst retrieval behaviour;
- avoid parallel polling loops designed to simulate streaming.

The CTP may throttle excessive API usage.

24. Duplicate Handling (REST Real-Time)

Where Users retrieve data from multiple regions or overlapping polling windows:

- duplicate records may be received;
- duplicate detection MUST use economic identifiers;
- publication timestamps MUST NOT determine uniqueness.

The duplicate identification principles defined in Section 10 apply equally to this interface.

25. Recovery and Reconciliation

Users MUST:

- detect gaps in retrieval;
- re-request missing data within supported time windows;
- ensure idempotent downstream processing.

The Real-Time CSV interface does not replace the Historical File interface for full-day backfill.

PART C - Historical File Collection (REST)

26. Historical Interface Overview

The Historical File interface provides complete, periodic datasets of CT data via secure REST-based file download.

This interface is intended for:

- end-of-day reconciliation;
- backfill;
- audit;
- research and analytics.

26.1. Endpoints and Environment Configuration

The Historical data interface is accessed via REST-based endpoints that are aligned with the Real-Time CSV interface.

The Historical interface uses the same API host as the Real-Time CSV service, with access differentiated solely by the resource path

Environment	Endpoint	IP Addresses	Path
UAT	https://data-api-uat.ets-connect.co.uk		/v1/bonds/historical/eod/<YYYY-MM-DD>
Production	https://data-api.ets-connect.co.uk	167.254.164.46 167.254.165.46	/v1/bonds/historical/eod/<YYYY-MM-DD>

26.2. Authentication and Authorization (Auth0)

Authentication and authorisation for the Historical interface SHALL be performed using Auth0 in accordance with Section 22.2.

All requirements relating to token acquisition, credential management, and request authentication apply equally.

27. File Availability and Publication Schedule

Historical files:

- are published on a defined UTC schedule;
- cover defined business-day periods;
- reflect full lifecycle state.

Users MUST align file processing to UTC boundaries.

28. File Integrity and Validation

Users MUST:

- verify file completeness;
- validate checksums (where provided);
- confirm record counts;
- detect corruption or truncation.

29. Historical Duplicate Handling

Historical files will contain:

- original trade records;

- Amend events;
- Cancel events.

Users MUST preserve lifecycle ordering and state integrity.

Duplicate handling MUST follow Section 10 principles where applicable.

30. Backfill and Replay Boundaries

Historical files provide authoritative full-day state.

Users MUST NOT rely on FIX replay beyond the current UTC day for historical completeness.

31. Operational Discipline (Historical)

Users MUST:

- avoid excessive download attempts;
- apply backoff when errors occur;
- avoid repeated full-day re-downloads without operational need.

32. Fair Use

The Historical interface is designed to support analytical, reconciliation, and research use cases.

To ensure platform stability and equitable access for all Users, the CTP applies fair use principles to historical data access.

Fair use controls are intended to prevent:

- repetitive downloading of identical datasets;
- excessive automated retrieval behaviour;
- disproportionate use of concurrent API sessions;
- activity that materially increases infrastructure load without corresponding analytical purpose.
- Users must ensure that their historical access patterns are efficient and proportionate to their legitimate use case.

Where usage materially exceeds reasonable operational norms, the CTP may:

- engage with the User to optimise behaviour;
- apply temporary rate controls;
- limit concurrent sessions;
- require batching or caching of repeated requests.

Fair use controls will be applied consistently across Users within the same licence category.

These controls are designed to protect service stability and ensure equitable access, and are not intended to restrict legitimate analytical or research activity.