VIXIO Regulatory Intelligence

TRUST CENTRE

PART A · V1.5

Trust Centre

Security, privacy, data processing, and AI commitments for procurement and compliance teams. A contractual instrument incorporated by reference into the Order Form and Terms and Conditions.

VIXIO Regulatory Intelligence

Compliance Online Limited · Registered in England and Wales No. 05706431

St Clare House, 30 Minories, London, EC3N 1DD

PUBLISHED AT TRUST.VIXIO.COM · SEPTEMBER 2026 · CONFIDENTIAL

TRUST CENTRE · PART A · V1.5

Vixio Trust Centre

Last updated September 2026 · v1.5 · Changelog

Overview

Security, privacy, data processing, and AI commitments for procurement and compliance teams. This Trust Centre is a contractual instrument incorporated by reference into the Order Form and Terms and Conditions.

Data Processing Agreement

Part B: DPA available for execution as an addendum to the Order Form.

Read →

AI Sub-processors Schedule

Part C: AI sub-processors, foundation models, and transfer mechanisms.

Read →

Privacy Policy

v2.0: UK GDPR & DPA 2018 governing personal data processing.

Read →

Certifications & assurance

ISO 27001:2022

Certificate 267181

Valid to 05 October 2028 · British Assessment Bureau · UKAS 8289

UK GDPR

Compliant

Privacy Policy v2.0 and DPA in place

SOC 2 Type II

Planned for Q1 2027

On roadmap, target certification Q1 2027

Cyber Essentials

Planned for Q4 2026

UK Government scheme, certification planned for Q4 2026

Quick reference contacts

TOPIC	CONTACT
Data protection	dataprotection@vixio.com
Security / vulnerability disclosure	tech@vixio.com
Support	support@vixio.com
General / legal	info@vixio.com

Document index

DOCUMENT	VERSION	LAST UPDATED
Part A: Trust Centre	v1.5	September 2026
Part B: Data Processing Agreement	v1.1	May 2026
Part C: AI Sub-processors Schedule	v1.1	May 2026
Privacy Policy	v2.0	May 2026
Acceptable Use Policy	v1.0.1	September 2026

A1. Introduction

Compliance Online Limited, trading as VIXIO Regulatory Intelligence, is the contracting entity for all services described in this Trust Centre. Vixio operates cloud-based regulatory intelligence platforms serving compliance teams in gambling, payments, and financial services.

This Trust Centre is the primary reference document for procurement, information security, legal, and compliance teams at subscriber organisations. It is a living document, updated when material changes occur. The version current at the date of your Order Form is the version incorporated into your subscription unless otherwise agreed in writing.

Security

Last updated September 2026 · v1.5 · Changelog

A2.1 Security Programme

Vixio maintains an Information Security Management System (ISMS) aligned to ISO/IEC 27001:2022, governed by a formal Information Security Policy reviewed annually. The ISMS covers all employees, contractors, suppliers, and stakeholders interacting with Vixio's information systems, data, or infrastructure, including personal devices under BYOD arrangements. Security responsibilities are designated within the technology team, with the CTO serving as ISMS Lead. Executive management provides leadership, budget, and oversight of ISMS objectives.

A2.2 ISO 27001 Certification

Standard	ISO/IEC 27001:2022
Status	Certified, active
Certificate number	267181
Issued by	British Assessment Bureau (Amtivo Group), UKAS accreditation 8289
Valid from	06 October 2025
Expiry date	05 October 2028 (subject to annual surveillance assessments)
Scope	Development, delivery, and ongoing operation of Vixio's cloud-based platforms and associated services, including the processing of customer, employee, and supplier information across infrastructure, endpoints, and SaaS systems.
Certificate	Available on request from tech@vixio.com

A2.3 Cyber Essentials

Scheme	UK Government Cyber Essentials
Status	Planned for Q4 2026
Certificate number	Not yet issued

A2.4 Infrastructure Security

- Encryption in transit (TLS 1.2 or higher) and encryption at rest for all cloud-hosted personal data.
- Network segmentation, firewall controls, and intrusion detection.
- Centralised logging, monitoring, and automated alerting.
- Regular vulnerability scanning and annual penetration testing by a qualified third-party provider.
- Cloud infrastructure hosted on Amazon Web Services (AWS) with enterprise-grade security controls.

A2.5 Access Controls

- Role-based access control (RBAC) across all environments.
- Multi-factor authentication (MFA) enforced for all Vixio staff on production systems.
- Privileged access management for infrastructure with quarterly access reviews.
- Single sign-on (SSO) available for enterprise subscribers.
- Principle of least privilege enforced.

Subscriber-side credential obligations, including the requirement that Users keep login details confidential and notify Vixio of suspected compromise, are set out in the Acceptable Use Policy.

A2.6 Vulnerability Disclosure

Report vulnerabilities to tech@vixio.com. Do not exploit, publicly disclose, or use the vulnerability against third-party systems. Provide sufficient information to reproduce the issue. For valid reports, Vixio will:

- Acknowledge receipt within 3 business days.
- Handle your report confidentially.
- Not take legal action against good-faith disclosures.
- Credit you on the disclosure unless you prefer otherwise.

A2.7 Incident Response

- Documented incident response procedure maintained and tested.
- Confirmed or suspected personal data breach notified to affected customers within 48 hours.
- Written incident report available on request following a confirmed breach.
- Ongoing remediation communications provided throughout the incident lifecycle.

Data Privacy

Last updated May 2026 · v2.0 · Changelog

This section summarises Vixio's privacy commitments. The full Privacy Policy (v2.0, May 2026) governs in the event of conflict and is incorporated by reference into the Terms and Conditions.

A3.1 Data Controller

Compliance Online Limited is the data controller of personal data collected from users in connection with the Services under UK GDPR and the Data Protection Act 2018. Data protection contact: dataprotection@vixio.com.

A3.2 Categories of Personal Data

CATEGORY	EXAMPLES
Identity	First name, last name, job title
Contact	Work email, telephone, address
Financial	Payment details (processed via third-party payment provider)
Technical	IP address, browser, login data, session identifiers, cookies
Usage	Pages visited, searches, VIQ prompts, feature interactions
Document content	Content of documents uploaded to the Workspace Document Library
AI interaction data	Prompts submitted to VIQ and SCANS, and associated metadata
Communications	Support ticket content, email correspondence
Marketing	Communication preferences

A3.3 Legal Bases for Processing

LEGAL BASIS	APPLIES TO
Consent (Art. 6(1)(a) UK GDPR)	Marketing communications
Contract performance (Art. 6(1)(b))	Service delivery, account management, AI features, Workspace
Legal obligation (Art. 6(1)(c))	Tax, regulatory compliance
Legitimate interests (Art. 6(1)(f))	Security, analytics, fraud prevention, service improvement

A3.4 Retention

Personal data is retained only as long as necessary for the purposes for which it was collected. Key retention periods:

Account and identity data	Duration of subscription plus 7 years
Financial and transaction data	7 years
Usage and technical data	Up to 24 months
VIQ and AI interaction data (prompts)	Up to 24 months (logged as usage data), then deleted
Workspace Document Library content	Duration of subscription, deleted within 30 days of termination
Aggregated and anonymised data	Retained indefinitely (does not identify individuals)

Full retention schedule in the Privacy Policy.

A3.5 Data Subject Rights

Data subjects have the following rights. Requests to dataprotection@vixio.com. Complaints to the ICO at ico.org.uk/concerns.

Access

Obtain a copy of personal data held about you.

Erasure

Request deletion of personal data, subject to applicable exceptions.

Portability

Receive personal data in a structured, machine-readable format.

Rectification

Correct inaccurate or incomplete personal data.

Restriction

Restrict processing in defined circumstances.

Objection

Object to processing based on legitimate interests or for direct marketing.

Automated decision-making

Rights relating to solely automated decisions producing legal effects.

A3.6 International Transfers

Transfers outside the UK are made only subject to appropriate safeguards: Standard Contractual Clauses (EU SCCs) with UK Addendum, or UK International Data Transfer Agreements. The applicable mechanism for each sub-processor is set out in Part C.

See the full Privacy Policy for complete detail.

Data Processing

Last updated May 2026 · v1.1 · Changelog

Where Vixio processes personal data on behalf of a customer organisation, a Data Processing Agreement is available for execution as an addendum to the Order Form.

A4.1 Data Processing Agreement

Where Vixio processes personal data on behalf of a customer organisation, a Data Processing Agreement (DPA) is available for execution as an addendum to the Order Form. The full DPA text is set out in Part B of this document set, published at trust.vixio.com. The DPA governs the relationship between Vixio as data processor and the customer as data controller.

A4.2 Nature & Location of Processing

Schedule B1 of the DPA sets out the particulars of processing. Customer personal data is stored and processed as follows:

ACTIVITY	DESCRIPTION
Storage	Customer personal data is stored within Vixio's cloud infrastructure (Amazon Web Services, UK/EU region) for the purpose of service delivery.
AI feature processing	Customer inputs (prompts and document content) and associated metadata are transmitted to AI sub-processors where AI functionality is used. Sub-processor locations and transfer mechanisms are set out below and in Part C.
Document ingestion and retrieval	Documents uploaded to the Workspace Document Library are stored in Vixio's AWS (UK/EU) infrastructure. Document content is called transiently into AI processing pipelines when AI functionality is used and is not persistently stored within AI sub-processor infrastructure.

A4.3 Sub-processors

The full sub-processor list, including AI sub-processors, is set out in Part C. Vixio provides not less than 30 days' written notice before adding a net-new sub-processor.

SUB-PROCESSOR	PURPOSE	LOCATION	TRANSFER MECHANISM
Amazon Web Services	Primary cloud infrastructure; Amazon Bedrock AI platform	EU / UK	EU SCCs + UK Addendum
Microsoft Azure	Azure OpenAI Service: managed AI model hosting	EU / UK	EU SCCs + UK Addendum
Google Cloud	Vertex AI platform: managed AI model hosting	EU / UK	EU SCCs + UK Addendum
Anthropic PBC (via AWS Bedrock)	LLM reasoning with Claude family models for VIQ and SCANS	USA (via AWS region)	EU SCCs + UK Addendum
OpenAI L.L.C. (via Azure)	LLM reasoning with GPT family models for evaluation and deployment	USA (via Azure region)	EU SCCs + UK Addendum
Pinecone	Vector database; semantic retrieval; AI orchestration	USA	EU SCCs + UK Addendum
Elasticsearch B.V.	Search indexing for keyword and structured search	EU	Adequacy

SUB-PROCESSOR	PURPOSE	LOCATION	TRANSFER MECHANISM
Glyphic AI	AI sales-call assistant: recording, transcription and analysis of customer calls	USA	EU SCCs + UK Addendum
Amplemarket	Sales engagement and outreach platform	USA	EU SCCs + UK Addendum

A4.4 AI and Data Use Policy

Key commitment: customer data is not used to train AI models for the benefit of other customers.

- Customer inputs, including prompts and document content, are not used to train foundation models for the benefit of other customers.
- AI sub-processors are contractually restricted from using customer data to train or improve models.
- AI services are accessed through enterprise-managed platforms (AWS Bedrock, Azure OpenAI, Google Vertex AI) with controlled execution environments and data isolation.
- Vector embeddings stored for semantic retrieval are derived representations. Original content is not stored in human-readable form within the vector database.
- Documents uploaded to the Workspace Document Library are processed transiently through AI pipelines and are not persistently stored within AI sub-processor infrastructure.

Restrictions on subscriber use of Service Data, including the prohibition on inputting Service Data into public AI models, are set out at Section 5 of the Acceptable Use Policy.

TRUST CENTRE

Platform Overview

Last updated September 2026 · v1.5 · Changelog

A contractual description of the three core components of the Vixio platform, for the benefit of procurement, compliance, and information security reviewers.

A6.1 Regulatory Intelligence Content

The Vixio content platform is a continuously updated regulatory intelligence resource, built and maintained by Vixio's in-house editorial and analyst team. It serves as the authoritative source of regulatory knowledge underpinning all three Vixio product lines (GamblingCompliance, PaymentsCompliance, and Financial Services) and provides the corpus from which VIQ draws its responses.

Horizon Scanning

A continuously updated feed of regulatory developments sourced from regulatory bodies, government agencies, and official publications. Covers new legislation, consultations, enforcement actions, guidance updates, and policy announcements.

Analyst Insights

Expert analysis from Vixio's specialist analyst team: outlook pieces, deep-dive analysis, practical how-to guides, and thematic research designed to contextualise raw regulatory data.

Regulatory Databases

Structured, searchable databases of regulations, requirements, and obligations, organised by jurisdiction and topic. Each entry links to the underlying legislative source.

Regulatory Library

A comprehensive library of primary source legislative and regulatory documents: legislation, rules, guidance, consultation papers, and official publications.

Content standard: all content is for information purposes only and does not constitute legal advice. Subscribers are responsible for verifying accuracy and applicability.

A6.2 Workspace: Legislative Change Management

Workspace is Vixio's user orchestration layer for regulatory and legislative change management. It enables compliance teams to move from awareness of a regulatory change through to assessment, task management, obligation mapping, and reporting, within a single integrated environment.

1 Triage

The entry point for regulatory change management. New regulatory developments land in Triage for review and categorisation.

- Inbound feed of regulatory developments from horizon scanning
- Relevance and materiality assessment workflow
- Routing to Boards or Regulatory Mapping
- Audit trail of triage decisions

2 Boards

A Kanban-style workflow tool for managing compliance workload and tasks arising from regulatory change.

- Kanban-style task and workload management
- Task creation, assignment, and deadline tracking
- Multi-workstream management across topics and jurisdictions
- Integration with Triage: tasks created from triage decisions

3 Regulatory Mapping

The structured compliance framework at the heart of Workspace, built from three integrated components:

- Legislation Library: curated subset of the Vixio Regulatory Library
- Obligations Library: specific obligations extracted from legislation
- Document and Policy Library: internal policy mapping to obligations

4 Reporting

Reporting and audit trail covering activities across all Workspace tools.

- Activity reporting across Triage, Boards, and Regulatory Mapping
- Audit trail of decisions, assignments, and changes
- Exportable reports for internal governance and external review

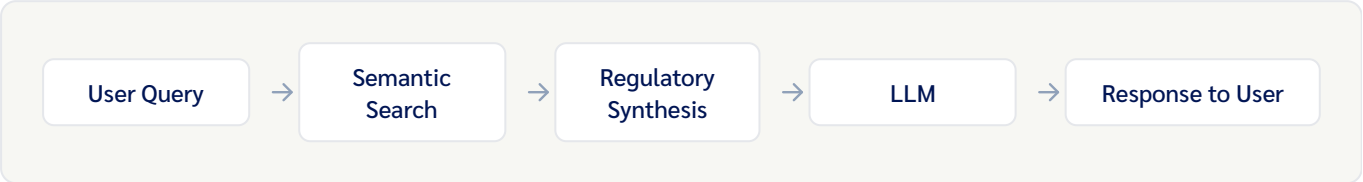
Packaging: Workspace is available in tiered packages. Inclusions, user permissions, and pricing are set out in the Order Form.

A6.3 VIQ: AI Regulatory Intelligence

VIQ draws exclusively from Vixio's proprietary regulatory corpus. It does not access the open internet. All responses are grounded in Vixio's editorial content.

How VIQ works

VIQ is a retrieval-augmented generation (RAG) system. When a user submits a query, VIQ performs a semantic search of Vixio's regulatory corpus to retrieve the most relevant content. That content is passed, with the user's query, to a large language model which generates a structured, natural language response.



Capabilities

Natural Language Queries

Ask regulatory questions in plain language across any jurisdiction and topic. VIQ returns structured responses with source references.

Regulatory Analysis

Structured analysis, summarisation, and comparison of regulatory requirements across jurisdictions and topics.

Classification and Q&A

Structured Q&A, classification of regulatory content, and extraction of specific requirements from Vixio's corpus.

Responsible use

Outputs are not legal advice	VIQ outputs are for information and research purposes only. Subscribers are responsible for verifying accuracy and applicability before relying on any output.
No training on customer data	Prompts and queries submitted to VIQ are not used to train foundation AI models for the benefit of other customers. Full commitments in A4.3 and Part C.
Human oversight	Vixio's editorial and analyst team maintains the regulatory corpus. VIQ outputs are not reviewed individually prior to delivery; subscribers are responsible for verification.

No automated decisions	Vixio does not use VIQ to make automated decisions that produce legal effects on or significantly affect subscribers.

Responsible AI

Last updated September 2026 · v1.5 · Changelog

A9.1 How VIQ Works

VIQ is a retrieval-augmented generation (RAG) system. User queries trigger semantic retrieval from Vixio's proprietary regulatory corpus via Pinecone vector search. Retrieved content is passed as context to a large language model (currently from Anthropic's Claude family, accessed via AWS Bedrock) to generate a response. The regulatory corpus, maintained by Vixio's editorial and analyst team, is Vixio's primary intellectual asset. VIQ does not access the open internet.

A9.2 Model Governance

Vixio operates a continuous model evaluation programme. The specific models deployed may change as Vixio evaluates and optimises across model releases. Model version changes within an approved sub-processor do not constitute the addition of a new sub-processor.

MODEL FAMILY	PROVIDER	STATUS
Claude	Anthropic (via AWS Bedrock)	Primary, in production
GPT	OpenAI (via Azure)	Under evaluation
Gemini	Google (via Vertex AI)	Under evaluation
Llama	Meta	Under evaluation
Mistral	Mistral AI	Under evaluation
Nova / Titan	Amazon (via AWS Bedrock)	Under evaluation

A9.3 Human Oversight

Vixio's editorial and analyst team provides human oversight of the regulatory corpus underpinning VIQ. VIQ outputs are not reviewed individually prior to delivery to subscribers. Subscribers are responsible for verifying the accuracy and applicability of outputs as set out in A6.3. Vixio does not use AI to make automated decisions that produce legal effects on subscribers.

A9.4 AI Operating Principles

- ✓ Customer data, including prompts and document content, is not used to train foundation models for the benefit of other customers.
- ✓ AI outputs are supplementary to, not a replacement for, professional regulatory and legal advice.
- ✓ Vixio does not use AI to make automated decisions producing legal effects on or significantly affecting subscribers.
- ✓ AI sub-processors are contractually restricted from training or improving models on customer data without explicit authorisation.
- ✓ Material changes to AI infrastructure affecting data processing will be notified to subscribers with not less than 30 days' notice.
- ✓ The AI sub-processor list and foundation model list are maintained at trust.vixio.com and updated when changes occur.

The contractual terms governing AI Functionality, ownership of Outputs, and your obligation to verify Outputs before relying on them are set out at Section 7 of the Acceptable Use Policy.

TRUST CENTRE

Compliance & Certifications

Last updated September 2026 · v1.5 · Changelog

ISO/IEC 27001:2022
Certified

UK GDPR / Data Protection Act 2018
Compliant

SOC 2 Type II
Planned for Q1 2027

Cyber Essentials
Planned for Q4 2026

Certification status

FRAMEWORK	STATUS	DETAIL
ISO/IEC 27001:2022	Certified	Certificate 267181, valid to 05 October 2028 (annual surveillance assessments)
UK GDPR / Data Protection Act 2018	Compliant	Privacy Policy v2.0 and DPA in place, published at trust.vixio.com
SOC 2 Type II	Planned for Q1 2027	On roadmap, target certification Q1 2027
Cyber Essentials	Planned for Q4 2026	UK Government scheme, certification planned for Q4 2026

ISO 27001:2022 detail

✓ Certified, active

Certificate number	267181
Issued by	British Assessment Bureau (Amtivo Group), UKAS accreditation 8289
Valid from	06 October 2025
Expiry	05 October 2028 (annual surveillance)
Scope	Development, delivery, and ongoing operation of Vixio's cloud-based platforms and associated services, including the processing of customer, employee, and supplier information across infrastructure, endpoints, and SaaS systems.

UK GDPR / Data Protection Act 2018

Compliance Online Limited is the data controller of personal data collected from users in connection with the Services. Vixio maintains a Privacy Policy (v2.0, May 2026) and a Data Processing Agreement governing personal data processing on behalf of customer organisations. International transfers are made under EU SCCs with UK Addendum or UK IDTAs as applicable. See the Data Privacy page for the summary, or the full Privacy Policy for complete detail.

SOC 2 Type II roadmap

- Planned for Q1 2027

SOC 2 Type II is on the Vixio compliance roadmap with a target certification date of Q1 2027. Vixio will publish observation period and auditor information when the programme commences.

Cyber Essentials detail

- Planned for Q4 2026

Scheme	UK Government Cyber Essentials
Certificate number	Not yet issued

Support & Availability

Last updated September 2026 · v1.5 · Changelog

A7.1 Service Availability

TARGET UPTIME

99.5%

monthly

Target uptime	99.5% monthly (excluding scheduled maintenance)
Planned maintenance	Notified in advance; scheduled outside core UK business hours where possible
Incident communication	Email notification to subscriber account contact
Status	Available via trust.vixio.com · contact support@vixio.com

A7.2 Support Tiers

SEVERITY	DEFINITION	RESPONSE TARGET
P1 · Critical	Platform entirely unavailable	Within 4 business hours
P2 · High	Major feature unavailable or severely degraded	Within 1 business day
P3 · Medium	Feature degraded but workaround available	Within 3 business days

SEVERITY	DEFINITION	RESPONSE TARGET
P4 · Low	General enquiry or minor issue	Within 5 business days

Support contact: support@vixio.com

A7.3 Escalation

Unresolved issues should be escalated to your named account manager or to info@vixio.com. Enterprise subscribers have a dedicated customer success contact.

A7.4 Training

Vixio offers onboarding and platform training for subscribers, including remote and on-site sessions at Vixio's discretion. Contact your account manager to arrange.

Acceptable Use Policy

Last updated September 2026 · v1.0.1 · Changelog

Document control

This Policy is the Acceptable Use Policy referred to in Condition 2.1 of the VIXIO General Terms and Conditions. It forms part of the Trust Centre and is incorporated into, and forms part of, the Agreement.

Contracting entity	Compliance Online Limited t/a VIXIO Regulatory Intelligence (Co. No. 05706431)
Registered address	7th Floor, St Clare House, 30 Minories, London, EC3N 1DD (per Condition 19.2 of the General Terms and Conditions)
Governing law	England and Wales (Condition 27.1); Delaware, USA where the Customer is established in the United States (Condition 27.2)
Applies to	Customer, Customer Users and Third Party Users under an Order incorporating the General Terms and Conditions
General / legal enquiries	info@vixio.com
Data protection	dataprotection@vixio.com
Security / vulnerability disclosure	tech@vixio.com

1. Purpose and Scope

1.1 This Acceptable Use Policy ("Policy") sets out the rules governing use of the Services by Compliance Online Limited, trading as VIXIO ("VIXIO", "we", "us", "our"). It applies to the Customer and all Users (being Customer Users and Third Party Users),

as those terms are defined in the Order and the VIXIO General Terms and Conditions (together, the “Agreement”).

1.2 This Policy is the “Acceptable Use Policy” referred to in Condition 2.1 of the General Terms and Conditions and forms part of the Trust Centre, together with the Documentation, the DPA, the Security Policy and the Service Levels. It is incorporated into, and forms part of, the Agreement.

1.3 The Customer must ensure that its Users comply with this Policy and remains liable for any breach of the Agreement, including this Policy, by its Users or by any third party using a User's log-in details (Condition 3.1(c)).

1.4 In the event of any conflict or ambiguity between this Policy and the other parts of the Agreement, the order of precedence at Condition 2.8 of the General Terms and Conditions applies: Special Terms, then the General Terms and Conditions, then the schedules (including this Policy), then the Order.

2. Definitions

2.1 Capitalised terms used in this Policy and not otherwise defined have the meanings given to them in the General Terms and Conditions, including “Customer”, “Customer Users”, “Third Party Users”, “Users”, “Client Content”, “Service Data”, “Services”, “Tier”, “Third Party Integration”, “Documentation” and “Trust Centre”.

2.2 “AI Functionality” and “Outputs” have the meanings given in Condition 8 of the General Terms and Conditions: AI Functionality means the artificial intelligence and machine learning functionality used by the Services to process Client Content and third party materials, and Outputs means the content generated using that functionality.

2.3 “Automated Access” means any method of accessing the Services other than direct, manual use by a User through the standard interface, or an authorised Third Party Integration, including scripts, bots, crawlers, scrapers and unauthorised application programming interface (API) calls.

3. General Principles

When using the Services, you must:

- comply with all applicable laws (Condition 4.3);

- ensure the number of Users, and your and their usage, does not exceed the limitations of your Tier (Condition 3.1);
- keep login details confidential and not share them with any individual who has not been assigned their own login details (Condition 3.3); and
- co-operate with any reasonable security or other checks or requests for information made by VIXIO (Condition 4.5).

4. Use of the Services

4.1 You must not, and must ensure your Users do not, access, store, distribute or transmit using the Services (Condition 4.2):

- any Virus;
- any material that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing, or racially or ethnically offensive;
- any material that facilitates illegal activity, depicts sexually explicit images, or promotes unlawful violence;
- any material that is discriminatory based on race, gender, colour, religious belief, sexual orientation or disability; or
- any material that is otherwise illegal or causes damage or injury to any person or property.

4.2 You must not, and must ensure your Users do not (Condition 4.3):

- try to gain unauthorised access to the Services or any connected networks, servers or computer systems;
- reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Services, except to the extent this restriction cannot be excluded by law;
- allow any employee of a third party, including a group company, to access the Services, other than as an authorised Third Party User;
- copy, download, scrape, store, publish, transmit, transfer, distribute, broadcast, circulate, sub-licence, bundle with other products, sell or otherwise use any portion of the Services or Service Data, other than sending Service Data to third parties as permitted under Condition 6; or
- use or access the Services to build or support, or assist a third party to build or support, products or services which compete with the Services.

4.3 We reserve the right, without liability, to disable your access to the Services if you breach Section 4.1 or 4.2 of this Policy.

5. Use of Service Data

5.1 You may use Service Data for your internal business purposes only. You may authorise Customer Users to share Service Data with a Third Party User on an individual basis, for your internal business purposes, provided such sharing is reasonable and proportionate. Widespread sharing, for example via an intranet or group email addresses, is not permitted unless otherwise agreed (Condition 6.1).

5.2 You must not, and must ensure your Users do not (Condition 6.2):

- download or store Service Data in any form other than its original form, or for any purpose other than as permitted under the Agreement;
- create a database or other collection or record, in electronic or hard copy form, by systematically downloading or storing Service Data, including bulk exports for future reference;
- create derivative works based on Service Data;
- use Service Data for any unlawful purpose;
- sub-licence, rent, lease, give access to, transfer or assign any rights in Service Data, except as permitted under Condition 6.1;
- alter or remove any copyright or other proprietary notices in Service Data;
- use Service Data to develop, offer for sale, or sell any product or service that competes with the Services; or
- input all or part of Service Data into any public large language model, machine learning model, foundation model, generative AI system, or other process commonly referred to as artificial intelligence, for any purpose including developing, improving, training, testing or supporting such a model or system, or to generate, synthesise or combine content.

5.3 The final restriction at Section 5.2 applies regardless of which Tier or Third Party Integration is used to access Service Data, and applies in addition to the AI Functionality provisions at Section 7 of this Policy.

6. Client Content

6.1 Where you upload or submit Client Content, you warrant that it will not (Condition 7.1):

- breach any law, statute or regulation, including data protection law;
- infringe the intellectual property or other legal rights of any person;
- be provided in breach of a legal duty owed to a third party, such as a contractual duty or duty of confidence;
- be deliberately or knowingly false, inaccurate or misleading; or
- give rise to any cause of action against VIXIO.

6.2 VIXIO does not actively monitor Client Content, but may delete Client Content it reasonably believes breaches Section 6.1 (Condition 7.2). VIXIO accepts no liability for Client Content and has no liability for errors or omissions in Service Data to the extent based on Client Content (Conditions 7.2 to 7.3).

7. AI Functionality Acceptable Use

7.1 What AI Functionality does

The Services use artificial intelligence and machine learning ("AI Functionality") to process Client Content and third-party materials and generate Outputs (Condition 8.1). The models in use, and the governance applied to them, are set out in Responsible AI.

7.2 Ownership of Outputs

You exclusively own all right, title and interest, including intellectual property rights, in Client Content and in Outputs generated using AI Functionality (Condition 8.1).

7.3 Accuracy and human oversight

VIXIO takes reasonable steps to monitor, test and evaluate AI Functionality, including periodic human review and controlling the materials to which it can refer, to help reduce material errors, bias and hallucinations (Condition 8.2). Outputs may nonetheless contain inaccuracies, omissions or bias, and are not warranted to be accurate, complete or error-free. You are responsible for reviewing all Outputs for accuracy, appropriateness, fitness for your intended purpose, and compliance with legal and regulatory requirements. All use of Outputs is at your own risk (Condition 8.3).

7.4 No training on Client Content

VIXIO will not use Client Content to train, fine-tune or otherwise improve any large language model, except to the extent strictly necessary to provide the Services. VIXIO may use aggregated, de-identified data derived from your use of AI Functionality to operate, improve and develop the Services, provided this does not identify you and does not include Client Content in a form that could be reverse engineered to identify you. Third-party AI providers and sub-processors used to support AI Functionality are bound by written obligations no less protective than this Policy, including a prohibition on using Client Content for training, fine-tuning or model improvement (Conditions 8.4 to 8.5).

7.5 Acceptable use of Outputs

You may use Outputs for your internal business purposes, consistent with Section 5 of this Policy. You must independently verify Outputs before relying on them for any business, compliance or regulatory decision.

8. Third Party Integration and Automated Access

8.1 The Services permit Third Party Integration. Availability, scope and number of Third Party Integrations depend on your Tier (Condition 5.1). You are responsible for the configuration, operation, security and maintenance of any integrated third-party software, platform, application or system, and must comply with the technical specification and requirements for integrations and APIs set out in the Trust Centre (Condition 5.3).

8.2 Automated Access to the Services, other than through an authorised Third Party Integration or direct manual use through the standard interface, is prohibited. This includes the use of bots, scripts, crawlers or scraping tools, consistent with the restriction on copying, downloading and scraping Service Data at Condition 6.2(b).

8.3 Any authorised Third Party Integration or API access must not:

- circumvent or attempt to circumvent rate limits, authentication requirements or other access controls;
- be used to build, populate or maintain a product, service or database that competes with the Services; or
- impose an unreasonable or disproportionate load on VIXIO's infrastructure.

9. Account and Credential Security

9.1 You must ensure Users keep their login details confidential and do not share them with any third party, and must inform VIXIO immediately if you have reason to believe a User's login details have become known to an unauthorised individual, or that the Services are being used, or are likely to be used, in an unauthorised way (Condition 3.3).

9.2 Customer Users must not be employed by any third party, including any other Affiliate, without VIXIO's prior written consent. Where the Customer acquires a new Affiliate or business (an “Acquisition”), employees related to that Acquisition may not be authorised as Users without VIXIO's prior written consent, which may be subject to additional Fees even where usage remains within the same Tier (Conditions 3.4 to 3.5).

10. Audit and Enforcement

10.1 VIXIO may audit your use of the Services on at least 30 days' prior written notice, conducted within normal business hours at VIXIO's expense, no more than once in any 12-month period except where required by law, a regulator, or where VIXIO reasonably believes you are in breach of the Agreement (Condition 4.5).

10.2 Where an audit reveals that a password has been provided to an individual who is not a User, or that Fees have been underpaid, VIXIO may suspend your access to the Services without liability and/or require payment of any underpayment and, at its sole discretion, an amount equal to the benefit received by the individual who is not a User (Condition 4.6).

10.3 VIXIO may suspend or terminate a User's account without liability if it reasonably believes that User is in breach of the Agreement (Condition 3.2), and may suspend or terminate the Agreement for reasonably believed fraudulent use, misuse or abuse of the Services, or failure to pay undisputed Fees (Condition 12.3).

11. Reporting Violations

If you believe this Policy has been breached, or wish to report a security vulnerability, please contact us using the details below.

General Policy concerns	info@vixio.com

Security vulnerabilities	tech@vixio.com · see the vulnerability disclosure commitments in Security
Data protection concerns	dataprotection@vixio.com

12. Policy Governance

Version	v1.0.1 (September 2026)
Owner	CPTO
Review cycle	Annually, or following a material change (for example new AI Functionality, integration, or automated access route)
Notice of material change	Not less than 30 days' prior written notice by email (Condition 10.1(b) of the General Terms and Conditions)
Related documents	Order; General Terms and Conditions; Documentation; DPA; Security Policy; Service Levels; Privacy Policy; Trust Centre