Consumer Switching Services Code

For submission to the Approved Code Scheme Board

Document Control

Title	Consumer Switching Services Code
Version	1.11
Status	Approved draft

Date of Issue	January 2026
Author/Owner	John Peerless Mountford (Code Lead)
Review frequency	Annual
Next review due	January 2027
Approved by	Group Board
Change log	See version control annex

Distribution List

- TPIs PCW
- Regulators
- Trade Associations
- Consumer Groups

Table of Contents

Code Sponsor

The Code Sponsor is responsible for:

- Maintaining, updating and publishing the Code
- Ensuring compliance with the Approved Code Scheme requirements
- Overseeing monitoring, audits and reporting
- Liaising with Regulators, ADR Bodies and consumer groups
- Ensuring impartiality and transparency in all Code related decisions

Governance and Oversight

The Dispute Resolution Ombudsman Board oversees the operation of the Code and shall

- Provide independent oversight of compliance and enforcement
- Review audit outcomes, sanctions and appeals
- Ensure decisions are free from conflict
- Maintain appropriate expertise across sectors
- Approve amendments to the Code and its annexes

Conflict of interest

Board Members must declare any actual or potential conflicts of interest. Where a conflict exists, the member shall recuse themselves from relevant decisions.

Mandatory Compliance Statement

Compliance with this Code is mandatory for all organisations accredited under the Consumer Switching Services Code. All requirements set out in the Code, including annexes and sector specific overlays, form binding conditions of accreditation and ongoing membership.

Scope of the Code

This Code applies exclusively to domestic consumers only. All businesses, SME, corporate or commercial contracts, tariffs or services are excluded, regardless of channel, presentation or supplier categorisation. Where a service or tariff is marketed to both consumer and business audiences, only the consumer facing elements fall within Code coverage. Any attempt to facilitate, promote, or switch business contracts under this Code is expressly prohibited.

Code Coverage

This CTSI code covers the role of third-party intermediaries across two key sectors with the intent to extend to cover to all sectors where consumers are introduced to products or services by a third party.

Active sectors

- Energy
- Water

Proposed sectors:

- Telecoms
- Insurance

Core Principles of the Code

The Code is built around seven foundational principles

- Principle 1: Transparency
- Principle 2: Code of Conduct
- Principle 3: Accessibility
- Principle 4: Data Protection
- Principle 5: Customer Experience
- Principle 6: Resource Training
- Principle 7: Operational Standard

These principles apply universally but are adapted to reflect the different markets through sector-specific overlays. Each sector has unique risks, regulatory frameworks, and client profiles. The Code uses modular annexes and mapping tables to link core principles to sector-specific obligations:

The Code

Purpose

To establish clear, enforceable, and adaptable standards for TPIs and PCWs serving domestic consumers. The Code promotes transparency, ethical conduct, accessibility, and layered compliance across multiple sectors.

Alignment with the Approved Code Scheme

This Code has been developed in accordance with the Core Criteria and Guidance of the Chartered Trading Standards Institute Approved Code Scheme.

The Code Sponsor commits to ensuring that the Code:

- Raises standards above minimum legal requirements
- Reduces detriment to consumers
- Promotes transparency and fairness
- Supports independent dispute resolution
- Provides clear, accessible information to all consumers and stakeholders

Legal framework

The Code operates alongside and above:

- Digital Markets, Competition and Consumers Act 2024
- Consumer Protection from Unfair trading Regulations2008
- Consumer Rights Act 2015
- UK GDPR and Data Protections Acy 2018
- Privacy and Electronic Communications Regulations 2003
- Sector specific regulations (Ofgem, Ofwat, Ofcom)

Principle 1: Transparency

1.1 **Supplier Relationships:** Code compliant organisations shall provide clear, prominent disclosure of all supplier relationships, commission structures, and commercial incentives before consumers begin any comparison process, with detailed breakdowns available on request.

1.2 **Whole Market Disclosure:** Code compliant organisations displaying potential services shall present a comprehensive view of available tariffs/rates. Where the organisation does not provide a whole-of-market view, this limitation shall be clearly and prominently disclosed. Prospective customers shall have the right to filter and sort results, with all filtering and ranking criteria transparently explained.

1.3 **Estimation Disclosure:** Code compliant organisations shall clearly disclose when estimates are used, provide appropriate caveats, and explain calculation methodologies including usage assumptions, data sources, and any limitations in accuracy.

1.4 **Cost Breakdown:** Code compliant organisations shall provide clear side-by-side comparisons of existing and proposed services including:

- All fixed fees, unit rates, and variable charges
- Estimated annual costs with clearly explained assumptions
- Contract terms and conditions differences
- Early termination fees and penalty clauses; and
- Service level commitments and performance guarantees

1.5 **Calculations:** Code compliant organisations shall maintain accurate, up-to-date customer data for calculations and provide, upon request, detailed explanations of their calculation methodologies, data sources, and any algorithmic processes used in comparisons.

1.6 **Disclosures:** Code compliant organisations shall, prior to any contract execution, disclose in writing:

- The exact commission amount and calculation method
- How commission may vary by supplier or product type
- Any bonuses or performance incentives received

- The impact of commission on the comparison ranking or presentation

1.7 **Recommendation Bias:** Code compliant organisations shall not prioritise suppliers based solely on commercial arrangements unless explicitly identified as sponsored content. All promoted listings must be:

- Visually distinct from organic results
- Clearly labelled as "sponsored," "promoted," or "advertisement"
- Segregated from unbiased comparison results; and
- Subject to the same accuracy and transparency requirements

1.8 **Eligibility:** Code compliant organisations shall validate all relevant customer identifiers and eligibility criteria before presenting comparison results or initiating any switching process, clearly explaining any validation failures or limitations.

1.9 **Supplier Objections:** Code compliant organisations shall handle supply transfer objections and switching issues transparently by:

- Clearly explaining the objection process and timeframes
- Proactively representing customer interests with suppliers
- Providing regular status updates during resolution; and
- Escalating unresolved issues to appropriate industry bodies

1.10 **Regionality:** Code compliant organisations shall clearly explain any geographical, infrastructure, or eligibility constraints including:

- Regional variations in pricing or service availability
- Postcode-specific limitations or surcharges
- Infrastructure requirements or restrictions; and
- Switching eligibility criteria and exceptions

1.11 **Default Tariff and Best Deal Identification:** Code compliant organisations shall clearly identify and explain:

- When customers are currently on default or standard variable tariffs.
- The potential savings available from switching.
- The best deals available based on customer circumstances; and

- Any temporary promotional rates and their expiry implications.

1.12 **Contract Terms Transparency:** Code compliant organisations shall provide clear, accessible summaries of key contract terms including:

- Contract duration and renewal terms.
- Price change mechanisms and notification periods
- Exit fees and cooling-off periods where applicable
- Service level agreements and compensation schemes; and
- Dispute resolution procedures.

1.13. **Contract duratio**n: Code compliant organisations shall clearly disclose contract duration and time of use eligibility in all comparisons. Any contract exceeding 24 months or showing business usage patterns shall be excluded from consumer presentation.

1.14 **Total Cost of Ownership Disclosure:** Code compliant organisations shall present total cost comparisons including:

- All direct costs (tariffs, standing charges, fees)
- Indirect costs (deposits, connection fees, equipment charges)
- Potential additional costs (excess usage, breach penalties); and
- Value-added services and their associated costs.

1.15 **Savings Claims Substantiation:** Code compliant organisations shall ensure all savings claims are:

- Based on verifiable customer data or clearly stated assumptions
- Presented with appropriate timeframes and caveats
- Inclusive of all relevant costs and fees; and
- Updated to reflect current market conditions and tariffs.

1.16 **Vulnerable Customer Identification:** Code compliant organisations shall clearly identify and explain:

- Special protections available for vulnerable customers

- Priority services and support mechanisms
- Tariffs or services specifically designed for vulnerable groups; and
- How vulnerability status may affect switching recommendations.

1.17. **Protection of deposits and prepayments:** Code compliant organisations must ensure that any deposits or pre-payments taken from consumers are protected through clear and transparent mechanisms.

Consumer must be informed in writing of

- The purpose of the deposit
- How it is held
- Refund conditions
- Any applicable statutory protections

Principle 2: Code of Conduct

2.1 **Selling Tactics:** Code compliant organisations shall not engage in pressure selling, impersonation, or misrepresentation.

2.2 **Sales Process:** Code compliant organisations shall record verbal sales interactions and retain them for dispute resolution. All details of calls including recordings are available upon request by the prospect or the customer.

2.3 **Documentation:** Code compliant organisations must assess contract suitability based on the prospect or customer-provided information and recommend the best available deals at the point the prospect intends to switch or take out a new agreement.

2.4 **Contractual Fairness:** Code compliant organisations must clearly explain all material contract terms, including separate charges where applicable and receive active consent from the prospect that they accept these either verbally or by tick box.

2.5 **Termination Fees:** Code compliant organisations must disclose any contract termination fees that may apply.

2.6. **Eligibility restrictions:** Code compliant organisations must validate consumer eligibility by excluding contracts that exceed permitted duration limits (normally 24 months unless explicitly regulated) or that show usage patterns inconsistent with domestic consumption. Contracts associated with business identifiers (VAT number, Company name, commercial premises, must not be promoted or facilitated under this Code.

2.7 **Authorisation to Act:** Code compliant organisations obtain formal written authorisation from consumers, including:

- Scope of authority
- Duration of authority
- Revocation procedures; and
- Consumer awareness of commission arrangements

2.8 **Independence and Impartiality:** Code compliant organisations shall demonstrate operational independence from suppliers where claims of impartiality are made, with clear governance structures preventing undue commercial influence on comparison results.

2.9 **Cooling Off Period:** Code compliant organisations must provide a 14-day cooling-off period.

2.10 **Summary Sheet:** Code compliant organisations shall provide a modular summary sheet of key contract terms at point of sale.

2.11 **Multi Language**: Code compliant organisations shall offer translated onboarding materials for non-English-speaking clients.

2.12. **Dealing with Consumers in their own home:** Code complaint organisations **do not conduct in home visits.** All consumer interactions take place remotely (e.g. online or by telephone). Should any organisation undertake in-home activity in the future, they must comply with the requirements of this Code including:

- Clear identification at the outset
- No pressure selling
- Provision of written information including cooling off rights
- Appropriate safeguarding of vulnerable consumers

Principle 3: Accessibility

3.1 **Vulnerability Accessibility:** Code compliant organisations must effectively identify and support vulnerable clients, including those with language barriers, cognitive impairments, or financial distress and ensure any services take this into account.

3.2 **Vulnerability Register:** Code compliant organisations shall inform the new supplier that their new customer is defined as vulnerable to ensure they are included in any vulnerable lists.

3.3 **Accessible Formats:** Code compliant organisations shall allow clients to be able to opt into preferred formats at no additional cost. (e.g. large print, Easy Read, translated versions), delivered via supplier partnerships. Additionally, prospects and customers shall be able to receive documentation in other languages.

3.4 **Accessibility Features:** Code compliant organisations shall include accessibility features in onboarding flows to identify clients with barriers.

3.5 **Signposting:** Code compliant organisations shall clearly signpost to independent advice services and

3.6 **Price Comparison Process:** Code compliant organisations shall provide simplified comparison options.

3.7. **Business Companion Vulnerability Guidance:** Code compliant organisations shall have regard to the Business Companion Consumer Vulnerability Guidance.

Principle 4: Data Protection

4.1 **Legal Compliance:** code compliant organisations shall process all personal data in strict accordance with applicable data protection legislation, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 ("PECR"), as amended from time to time.

4.2 **Consent Management:** Code compliant organisations shall obtain explicit, informed, and freely given consent before:

- Sharing personal data with suppliers, partners, or third parties
- Processing data for marketing purposes beyond the original comparison services
- Using personal data for profiling or automated decision-making; and
- Transferring data outside the UK/EEA.

4.3 Marketing Communications Control: prospects and clients must be able to:

- Opt-out of all marketing communications at any stage through clear, accessible mechanisms
- Manage communication preferences granularly by channel and content type
- Receive confirmation of opt-out requests within 2 working days; and
- Have their preferences respected across all group companies and partners

4.4 Data Security Measures: code compliant organisations shall implement and maintain appropriate technical and organisational security measures including:

- Role-based access controls with regular review and updating
- Encryption of personal data in transit and at rest
- Regular security assessments and penetration testing; and
- Staff training on data security and incident response procedures

4.5 Data Protection Governance: code compliant organisations shall maintain regularly updated, version-controlled data protection policies with a designated Data Protection Officer whose contact details are prominently displayed on the website and readily accessible to data subjects.

4.6 Data Minimisation and Purpose Limitation: code compliant organisations shall ensure that personal data collected is:

- Limited to what is necessary for the specified comparison services
- Used only for the purposes clearly communicated to the data subject
- Not processed for incompatible secondary purposes without additional consent; and
- Regularly reviewed to ensure continued necessity and relevance

4.7 **Data Retention and Deletion:** code compliant organisations shall establish and implement clear data retention policies specifying:

- Maximum retention periods for different categories of personal data
- Automatic deletion processes for data no longer required
- Secure destruction methods for deleted data; and
- Regular auditing of retained data to ensure compliance with retention limits.

4.8 **Data Subject Rights:** code compliant organisations shall provide clear, accessible procedures for data subjects to exercise their rights in compliance with the timescales prescribed by data protection legislation including:

- Access to their personal data within one month of request
- Rectification of inaccurate or incomplete data
- Erasure of data where legally permissible
- Data portability in commonly used formats; and
- Objection to processing based on legitimate interests.

4.9 **Third-Party Data Sharing Transparency:** code compliant organisations shall maintain and publish:

- Clear lists of all third parties who may receive personal data
- The purposes for which data is shared with each third party
- The legal basis for each type of data sharing; and
- How individuals can control or object to specific sharing arrangements.

4.10 **Privacy by Design and Default:** Code compliant organisations shall implement privacy by design principles ensuring:

- Data protection considerations are integrated into all new systems and processes
- Default settings provide maximum privacy protection for users
- Privacy impact assessments are conducted for new processing activities; and
- Regular reviews of existing systems to identify privacy enhancement opportunities

4.11 **Data Breach Management:** Code compliant organisations shall establish comprehensive data breach response procedures including:

- Detection and assessment processes with defined timescales
- Notification to supervisory authorities within 72 hours where required
- Communication to affected individuals without undue delay where high risk exists
- Documentation of all breaches and remedial actions taken; and
- Regular testing of breach response procedures

4.12 **Cross-Border Data Transfers:** code compliant organisations shall ensure that any international transfers of personal data:

- Are subject to appropriate safeguards as required by UK data protection law
- Include adequate protection mechanisms such as Standard Contractual Clauses
- Are clearly disclosed to data subjects with information about destination countries; and
- Are regularly reviewed to ensure ongoing adequacy of protection measures.

4.13 **Automated Decision-Making and Profiling:** code compliant organisations shall ensure that any automated decision-making or profiling:

- Is clearly disclosed to data subjects with information about the logic involved
- Provides meaningful information about the consequences for the individual
- Offers the right to human intervention and to contest automated decisions; and
- Is subject to regular testing for bias and discriminatory outcomes.

4.14 **Data Protection Impact Assessments:** code compliant organisations shall conduct Data Protection Impact Assessments for:

- New comparison services or significant changes to existing services
- Implementation of new technologies that process personal data
- Processing activities that may result in high risk to individuals; and
- Any processing involving vulnerable individuals or sensitive data categories.

Principle 5: Customer Experience

5.1 **Auditing:** Code compliant organisations shall participate in independent audit schemes and publish annual compliance statements with any audit undertaken. The compliance statement should include metrics on supplier coverage, complaints, and accessibility. This statement shall be recorded on the website.

5.2 **Complaints Procedure:** Code compliant organisations shall maintain a clear, accessible complaints procedure with defined response times (maximum 5 working days for acknowledgment, 20 working days for resolution) and escalation routes to the ADR scheme operated by Dispute Resolution Ombudsman.

5.3 **Website:** Code compliant organisations shall have a website including their contractual terms, registered office and details, complaint process, audit reports and data protection registration.

5.4 **Procedures:** Code compliant organisations shall maintain robust complaints procedures that are:

- Available online and in hardcopy
- Version-controlled with historical versions available; and
- Accessible via multiple channels e.g. phone, post, email

5.4. **Records:** Complaint records must be:

- Logged electronically with comprehensive details
- Updated regularly with actions taken; and
- Retained for minimum 6 years.

5.5 **Record Recording:** Code compliant organisations should implement compliance monitoring processes including:

- Evidence retention procedures
- Regular monitoring of sales activities against code requirements; and
- Telephone recording for compliance purposes (where applicable).

5.6 **Transparency:** Code compliant organisations shall ensure the switching or sign-up process is clear and transparent. Also, if there is an issue what is the resolution process.

Principle 6: Resource Training

6.1 **Training Requirements:** Code compliant organisations shall ensure all staff, agents, and third parties receive comprehensive and appropriate initial training and regular refresher training on code requirements, including consumer protection obligations, data handling procedures, and complaint resolution processes.

6.2 **Training Logs:** Code compliant organisations shall maintain detailed training logs tracking:

- Staff member details and roles
- Training completion dates and assessment results
- Renewal requirements and compliance status
- Training topics covered including code updates
- Competency assessments and remedial training records; and
- Training provider credentials and course approvals

6.3 **Training Frequency:** Code compliant organisations shall ensure training is refreshed annually as a minimum, with additional training triggered by code updates, regulatory changes, or identified competency gaps. All training records shall be retained for a minimum of three years for audit purposes.

6.4 **Competency Assessment:** Code compliant organisations shall implement regular competency assessments for all consumer-facing staff and technical personnel, with clear performance standards and remedial training procedures for those not meeting required standards.

6.5 **Technical Competency Requirements:** Code compliant organisations shall ensure technical staff possess appropriate qualifications and competencies in data management, comparison algorithms, website functionality, and cybersecurity relevant to their roles in operating comparison services.

6.6 **Consumer Service Competency:** Code compliant organisations shall ensure customer service staff are trained and competent in:

- Understanding comparison methodologies and limitations
- Explaining commercial relationships and potential conflicts of interest

- Identifying and supporting vulnerable consumers
- Data protection and privacy requirements; and
- Complaint handling and escalation procedures.

6.7 **Management Oversight and Competency:** Code compliant organisations shall ensure management personnel responsible for code compliance possess appropriate qualifications, experience, and ongoing professional development in consumer protection, regulatory compliance, and industry best practices.

6.8 **Third-Party and Supplier Relationship Management:** Code compliant organisations shall ensure staff responsible for supplier relationships are trained in:

- Contract management and performance monitoring
- Due diligence procedures for new suppliers
- Conflict of interest identification and management; and
- Commercial arrangement documentation and disclosure.

6.9 **Data Protection and Security Competency:** Code compliant organisations shall ensure relevant staff maintain current competency in:

- GDPR and data protection regulations
- Cybersecurity best practices and threat awareness
- Consumer data handling and consent management; and
- Incident response and breach notification procedures.

6.10 **Regulatory and Compliance Competency:** Code compliant organisations shall ensure compliance staff maintain current knowledge of:

- Relevant financial services regulations
- Consumer protection legislation
- Advertising and marketing standards; and
- Industry codes and guidance from regulatory bodies.

6.11 **Training Documentation and Verification:** Code compliant organisations shall maintain comprehensive training materials that are:

- Regularly updated to reflect code changes and regulatory updates

- Accessible to all relevant staff in appropriate formats
- Subject to independent verification of accuracy and completeness; and
- Approved by qualified training professionals or industry experts.

6.12 **Continuous Professional Development:** Code compliant organisations shall establish continuous professional development programs ensuring staff maintain current industry knowledge.

Principle 7: Operational Standards

7.1 **Representation:** code compliant organisations shall not misrepresent supplier availability, pricing, or service status unless reasonable evidence exists of current market conditions and supplier capacity.

7.2 **Ensure Up to Date Suppliers Lists:** code compliant organisations shall ensure when supplier authorisation is revoked or suspended, organisations must promptly inform all relevant parties including consumers with active comparisons and remove affected suppliers from active listings within 24 hours.

7.3 **Document Control:** code compliant organisations shall maintain version-controlled documentation of all procedures, comparison methodologies, and ranking algorithms, making historical versions available upon request to regulatory bodies and consumers.

7.4 **Plain English:** code compliant organisations shall ensure all consumer facing documentation, comparison tables, and service descriptions are in plain English with clear explanations of how comparisons are conducted, what factors influence rankings, and any commercial relationships affecting results.

7.5 **Pricing Data:** code compliant organisations shall maintain accurate, up-to-date supplier information and pricing data, with refresh cycles clearly disclosed to consumers and maximum data age limits established for different product categories.

7.6. **Exclusion logic:** Code compliant organisations must exclude any request for services that includes business identifiers such as VAT Registration, Company name or commercial premises.

Annex A: Legal Mapping

General Consumer Protection

Code provision	Legal basis	Notes
Transparency of pricing, commission and filtering	Digital Markets, Competition & Consumers Act 2024, DMCCA, Consumer Protection from Unfair Trading 2008, CPUTS,	Covers misleading omissions and commercial practices
No impersonation or pressure selling	Consumer Rights Act 2015 DMCCA & CPUTS	Aligns with unfair contract terms and aggressive selling practices
ADR Membership and complaint handling	Alternative Dispute Resolution for Consumer Disputes (Competent Authorities and Information) Regulation 2015	Required for code approval
Accessibility for vulnerable consumers	Equality Act 2010, Consumer Duty (FCA)	Applies to format switching, flags and inclusive onboarding

Contract duration	Consumer Rights Act 2015, Ofcom broadband rules	Prevents long term lock in
Time of use validation	Ofgem supply licence conditions, Equality Act 2010	Ensures domestic consumption patterns only

Energy Sector

Code provision	Legal basis	Notes
Supplier relationship disclosure	Ofgem TPI principles, Supply Licence Conditions (SLC)	Must declare commercial risks and commission structures
Tariff accuracy and filtering logic	Ofgem Confidence Code SLC -Price Cap	Filtering must not lead or exclude regulated tariffs
Vulnerability logic and switching safeguards	Priority Services Register, SLC	Must identify and protect vulnerable consumers during switching

Water Sector

Code provision	Legal basis	Notes
Switching safeguards and consent	Water Retail Markets Codes, GDPR	Consent and data handling during switching

Vulnerability and format switching	Ofwat vulnerability guidance, Equality Act 2010	Format switching and accessibility logic

Telecoms Sector

Code provision	Legal basis	Notes
Disclosure of commercial relationships	Ofcom General Conditions	Must declare commission and supplier links
Tariff comparison accuracy	Ofcom Price comparison, Guidance, CRA 2015,	Filtering logic must be fair, accurate and not misleading
Vulnerable consumer support	Ofcom Vulnerability guidance, Equality Act 2010	Format switching and inclusive onboarding

Price Comparison Websites (PCW)

Code provision	Legal basis	Notes
Ranking and filtering transparency	CMA PCW principles, DMCCA, CPUTS	Must disclose ranking logic and commercial influence
Supplier inclusion /exclusion logic	CMA PCW protection, DMCCA, CPUTS	Must not mislead by omitting suppliers without disclosure
Accessibility and format switching	CMA Guidance, Equality Act 2010, EHRC Code	Applies to all PCW interfaces and onboarding

Annex B: Customer Service Standards

Purpose

This annex sets out the minimum customer service standards required under this Code.

These standards apply to all TPIs and PCWs and must be embedded into day-to-day operations, staff training, and quality assurance processes.

General Service Standards

Professional Conduct

Organisations must ensure that all customer interactions are:

- Courteous
- Professional
- Accurate
- Free from pressure or manipulation

Responsiveness

Organisations must:

- Acknowledge enquiries within 2 working days
- Provide a substantive response within 5 working days
- Notify customers where additional time is required

Multi-Channel Access

Organisations must provide at least:

- A telephone contact number
- An email address
- A web-based contact form
- A postal address

Transparency of Identity

All communications must clearly identify:

- The organisation's name
- The representative's name
- The purpose of the contact

Pre-Contract Information Standards

Clarity of Information

Before a customer makes any decision, organisations must provide:

- A clear explanation of the service
- Any fees or commissions
- Whether the service is whole-of-market or restricted
- Any commercial relationships influencing recommendations

Quote Presentation

Quotes must:

- Be presented in a standardised format
- Include total cost of ownership
- Identify assumptions or estimates
- Highlight any exclusions

Suitability Explanation

Where a recommendation is made, organisations must explain:

- Why the option is suitable
- Any risks or limitations
- Any cheaper or simpler alternatives

Complaint Handling Standards

Purpose

Organisations must operate a fair, accessible, and effective complaints process.

Accessibility

The complaints process must be:

- Published on the website
- Available in writing on request
- Provided in accessible formats

Complaint Acknowledgement

Complaints must be acknowledged within 2 working days.

Final Response

A final response must be issued within 10 working days, unless:

- The complaint is complex
- Additional evidence is required

Where more time is needed, the customer must be informed.

Escalation Pathway

The complaints process must include:

- Stage 1: Initial investigation
- Stage 2: Senior review
- Stage 3: ADR referral

ADR Signposting

Final response letters must:

- Explain the customer's right to ADR
- Provide the ADR provider's details
- State that ADR is independent and free at the point of use

Record Keeping

Organisations must retain:

- Complaint logs
- Correspondence
- Evidence
- Final responses

for a minimum of 6 years.

Customer Communication Standards

Plain English

All communications must be:

- Clear
- Concise
- Free from jargon
- Free from misleading terminology

Confirmation of Key Decisions

Organisations must provide written confirmation of:

- Quotes
- Recommendations
- Switching instructions
- Contract acceptance

Notification of Errors

Where an error is identified, organisations must:

- Notify the customer promptly
- Explain the impact
- Provide corrective action
- Offer redress where appropriate

Website Standards

Mandatory Website Information

Websites must display:

- Company name and registration
- Contact details
- Complaints procedure
- ADR access information
- Privacy notice
- Cookie policy

Comparison Transparency

Where comparisons are provided, websites must:

- Explain ranking logic
- Identify sponsored listings
- State whether results are whole-of-market
- Provide clear assumptions

Accessibility Requirements

Websites must:

- Meet recognised accessibility standards
- Provide alternative formats on request
- Avoid dark patterns or misleading design

Customer Feedback and Continuous Improvement

Feedback Collection

Organisations must collect feedback through:

- Surveys
- Post-interaction reviews
- Complaint analysis

Trend Analysis

Feedback must be analysed to identify:

- Recurring issues
- Training needs
- Process improvements

Governance Reporting

Customer service performance must be reported to the Governance Board annually.

Evidence Requirements

Organisations must retain evidence of:

- Customer interactions
- Quotes and recommendations
- Complaint handling
- ADR outcomes
- Training records

Evidence must be available for audit on request.

Annex C: Independent Dispute Resolution Scheme

Purpose

This annex sets out the independent dispute resolution arrangements available to business customers where a complaint cannot be resolved through the code compliant organisations internal process.

The scheme provides:

- A fair, impartial and transparent process
- A binding outcome on the code compliant organisation
- A free point at the point of use service for eligible customers
- A structure pathway for conciliation and adjudication

Eligibility for ADR

Customers may access the Dispute Resolution Ombudsman service if:

- They have followed the code compliant organisations' internal complaints procedure
- They have received a final response letter, or
- 4 weeks have passed since the initial complaint without resolution
- The complaint relates to services covered by this Code; and
- The complaint is made within 12 months of the final response.

A case will not be considered if the:

- Complaint is already being dealt with by courts or other ombudsman schemes
- Claim exceeds the scheme's financial limits
- Matter is outside the scope of this Code; and
- Complaint is made more than 12 months after the final response.
- The case will be referred to an Adjudicator
- Both parties can submit further evidence and arguments
- The adjudicator will make a binding decision; and
- The decision will be issued within 40 days of complete case file receipt
- Customers retain the right to pursue legal remedies outside the scheme, but participation in the scheme does not require legal representation

Initial Application

To use the Dispute Resolution service, customers should:

- Complete an application form with supporting evidence
- Provide copies of all relevant correspondence
- Specify the expected outcome; and
- Submit within the required timeframes.

ADR Signposting requirements

Mandatory Signposting

Code compliant organisations must clearly signpost ADR:

- In the published complaints procedure
- In the Final response letters
- On their website
- In any communication closing a complaint

Required wording

Signposting must state that ADR:

- Is independent
- Is free at the point of use for eligible customers
- Decisions are binding on the code compliant organisation
- Can be accessed online or in writing

Accessibility

ADR information must be available in:

- Plain English
- Accessible formats on request
- Digital and non-digital channels

ADR Process Overview

The ADR process consists of:

- Conciliation
- Adjudication
- Binding decision
- Implementation and redress

Conciliation stage

Purpose

Conciliation aims to resolve the dispute informally and promptly.

Process

DRO will:

- Review the complaint
- Request evidence from both parties
- Facilitate communication
- Seek a mutually acceptable resolution

Timescales

Conciliation should normally conclude within **10 working days.**

Outcomes

Possible outcomes include:

- The issue of an apology
- Correction of errors
- Contract clarification
- Goodwill gestures
- Agreement to proceed to Adjudication

Adjudication Stage

Purpose

Adjudication provides a formal, independent assessment of the complaint.

Evidence Requirements

DRO may request

- Quotes
- Call Recording
- Emails and correspondence
- Contract documents
- System logs
- Data access records

Decision criteria

The Adjudicator will consider:

- The provisions of this Code
- Relevant laws and regulations
- Evidence provided
- Fairness and reasonableness

Timescales

Adjudication should normally be concluded within **20 working days.**

Binding decisions

Nature of decision

he Adjudicators decision is:

- **Binding** on the organisation
- **Not binding** on the customer, who may choose alternative remedies

Remedies

Remedies may include:

- Correction of errors
- Recalculation of charges
- Contract withdrawal or amendment
- Compensation for direct loss
- An apology or service improvement commitments
- Financial compensation up to £10,000 per case
- Payment of reasonable costs and inconvenience (maximum £500)
- That the Registered Member issues a written apology to the customer.

Implementation

Code compliant organisations must implement decisions within 28 days, unless otherwise specified.

Publication of outcome

Transparency

DRO may publish:

- Anonymised case summaries
- Thematic reports
- Trends and systemic issues

Purpose

Publication supports:

- Transparency
- Learning
- Continuous improvement

Evidence and cooperation requirements

Duty to cooperate

Code compliant organisations must:

- Provide evidence promptly
- Respond to DRO requests
- Not obstruct or delay the process

Evidence integrity

Evidence must be:

- Complete
- Accurate
- Unaltered
- Provide in the request format

ADR Fees

Where applicable, ADR fees may be

- Charged to the code compliant organisation
- Recovered via compliance levies
- Structured according to case volume or complexity

Customer costs

ADR is free at the point of use for eligible business customers.

Escalation beyond ADR

Referrals

Where systemic issues are identified, DRO may refer matters to the appropriate enforcement body and advise other Approved Code scheme sponsors.

Legal advice and adjudication independence

The adjudicators decision shall be based solely on the merits of the case, the evidence presented, and the Code's standards:

- Customers may seek independent legal advice at any stage of the dispute process
- The act of seeking legal advice shall not influence, delay, or alter the Adjudicators decision
- Adjudicators shall remain impartial and not consider external legal commentary unless formally submitted as evidence
- Customers retain the right to pursue legal remedies outside the scheme, but participation in the scheme does not require legal representation

Closure of ADR cases

ADR cases may be closed where:

- A binding decision has been issued
- The customer withdraws the complaint
- The organisation implements the remedy
- The complaint is outside scope
- The customer does not engage with the process

Annex D: Compliance & Monitoring

Purpose

This annex sets out the compliance, monitoring, audit and reporting requirements that code compliant organisations must meet to remain certified under this Code. It ensures

- Consistency of standards
- Transparent oversight
- Evidence-based assurance
- Continuous improvement
- Alignment with the Approved Code scheme

Compliance with the Code

Code compliant organisations must comply with all

- Seven foundation principles
- Annexes
- Sector specific overlays
- Instructions issued by the Code Sponsor/Governance Board

Compliance Statement

Code compliant organisations must submit an Annual Compliance statement confirming:

- Adherence to the Code
- Completion of required training
- Accuracy of published information
- Complaint and ADR performance
- Any material changes in ownership, structure or operations

Material changes Notification

Code compliant organisations must notify the Code Sponsor within 10 working days of:

- Insolvency or Administration
- Significant ownership changes
- Major operational failures
- Data breaches
- Regulatory enforcement action

Monitoring Activities

Monitoring Framework

The Code Sponsor shall operate a structured monitoring framework including:

- Annual compliance reviews
- Thematic reviews
- Spot checks
- Complaint trend analysis
- ADR outcome analysis

Evidence Requirements

Organisations must provide:

- Quotes
- Call recordings
- Contracts
- Complaint logs
- ADR correspondence
- Training records
- Data access logs

Continuous Improvement Logic

The Code Sponsor shall:

- Analyse monitoring outcomes
- Identify systemic issues
- Recommend improvements
- Update the Code where required
- Publish "You Said, We Did" summaries

Audit Requirements

Types

Audits may be:

- Annual
- Thematic
- Triggered (e.g., following a breach)
- Random

Scope

Audits may cover:

- Sales practices
- Data protection
- Complaint handling
- ADR cooperation
- Training and competency
- Website transparency
- Supplier engagement
- Operational resilience

Cooperation

Organisations must:

- Provide access to systems and records
- Respond to audit queries promptly
- Not obstruct or delay audits

Outcomes

Audit outcomes may include:

- Full compliance
- Partial compliance
- Non-compliance
- Serious breach

Outcomes will determine sanctions under Annex E.

Reporting & Transparency

Reporting to the Approved Code Scheme (CCAS)

Reporting Obligations

The Code Sponsor shall provide periodic reports to the Approved Code Scheme including:

- Annual compliance summaries
- Audit outcomes
- Complaint and ADR statistics
- Significant breaches
- Enforcement actions
- Continuous improvement updates

Format and Frequency

Reports shall be provided:

- In the format required by CCAS
- At the frequency required by CCAS
- With supporting evidence when requested

Transparency

The Code Sponsor may publish:

- Annual Code performance reports
- Thematic findings
- Improvement actions

Stakeholder Engagement

Feedback Mechanism

The Code Sponsor shall maintain structured feedback channels for:

- Business customers
- TPIs and PCWs
- Suppliers
- Regulators
- ADR bodies
- Industry associations

Use of Feedback

Feedback shall be used to:

- Identify emerging risks
- Improve Code content
- Enhance monitoring

- Inform training requirements

Data and Record Retention

Retention Periods

Organisations must retain:

- Complaint records. 6 years
- ADR records 6 years
- Contract records 6 years
- Letters of Authority 2 years
- Training records 3 years
- Audit evidence 3 years

Secure Storage

Records must be:

- Securely stored
- Accessible for audit
- Protected from unauthorised access

Publication and Transparency

Public Register

The Code Sponsor shall maintain a public register of:

- Code compliant organisations
- Suspended organisations
- Removed organisations

Publication of Breaches

The Code Sponsor may publish:

- Anonymised breach summaries
- Enforcement actions
- Systemic issues

Website Requirements

Organisations must publish:

- Their certification status
- Complaints procedure
- ADR access information

Non-Compliance and Escalation

Identification of Non-Compliance

Non-compliance may be identified through

- Audits
- Complaints
- ADR outcomes
- Monitoring
- Supplier feedback
- Regulatory referrals

Escalation Pathway

Non-compliance shall be escalated in accordance with Annex E.

Annex E: Sanctions & Standards

Purpose

This annex sets out the sanctions and enforcement framework that applies where an organisation fails to comply with this Code.

It ensures:

- Fair and transparent enforcement
- Proportionate and consistent sanctions
- Protection of business customers
- Integrity of the Approved Code Scheme
- Accountability for TPIs and PCWs

Principles of Enforcement

Fairness

Sanctions must be applied fairly, consistently, and proportionately.

Transparency

The organisation must be informed of:

- The nature of the breach
- The evidence relied upon
- The proposed sanction
- Their right to respond
- Their right to appeal

Proportionality

Sanctions must reflect:

- Severity of the breach
- Impact on customers
- Intent or negligence
- Repetition or systemic issues
- Cooperation with investigations

Independence

Enforcement decisions shall be overseen by the Governance Board or an appointed independent panel.

Types of Breach

Breaches may include:

- Failure to comply with any section of this Code
- Misleading or aggressive practices
- Data protection failures
- Failure to cooperate with audits or ADR
- Misuse of the Approved Code Scheme logo
- Repeated customer detriment
- Systemic operational failures
- Failure to notify material changes
- Obstruction of monitoring or investigation

Sanctions Framework

Sanctions may include one or more of the following:

Advisory Notice

Issued for minor breaches requiring corrective action.

Improvement Plan

A structured plan requiring:

- Specific actions
- Timescales
- Evidence of completion

Enhanced Monitoring

Additional audits, reporting, or oversight for a defined period.

Formal Warning

Issued where breaches are repeated or more serious.

Suspension

Temporary removal from the Code where:

- Serious breaches occur
- Improvement plans are not completed
- Customers are at risk
- Evidence is withheld

Suspended organisations must immediately cease use of all Code branding.

Removal from the Code

Permanent removal may occur where:

- Serious or systemic breaches persist
- There is deliberate misconduct
- There is misuse of the Approved Code Scheme logo
- The organisation fails to cooperate with investigations
- Insolvency or cessation of trading occurs

Referral to Regulators or Enforcement Bodies

Where appropriate, matters may be referred to:

- Trading Standards
- Regulators (Ofgem, Ofwat, Ofcom, FCA)
- Law enforcement

Investigation Process

Notification

The organisation will receive written notice of:

- The alleged breach
- Evidence held
- Required response times

Evidence Gathering

The Code Sponsor may request:

- Call recordings
- Contracts
- Complaint logs
- ADR correspondence
- Training records
- Website evidence
- Data access logs

Decision Making

Decisions shall be based on:

- Evidence
- Severity
- Customer impact
- Cooperation
- Previous compliance history

Communication of Outcome

The organisation will receive:

- A written decision
- Details of sanctions
- Required action
- Appeal rights

Appeals Process

Right to Appeal

Organisations may appeal sanctions within 10 working days of receiving the decision.

Grounds for Appeal

Appeals may be based on:

- Procedural error
- New evidence
- Disproportionate sanction
- Incorrect interpretation of the Code

Appeal Panel

Appeals shall be reviewed by:

- The Governance Board; or

- An independent review panel appointed by the Code Sponsor

Final Decision

The appeal decision is final.

Approved Code Scheme Logo Usage

Conditions of Use

Code compliant organisations may display the Approved Code Scheme logo only:

- While fully compliant with this Code
- In approved format
- In approved contexts
- In accordance with branding rules

Prohibited Uses

The logo must not be:

- Used by suspended or removed organisations
- Altered or modified
- Used in relation to services not covered by this Code
- Used in a way that misleads customers

Misuse of the Approved Code Scheme Logo

Misuse of the logo constitutes a serious breach.

Misuse includes:

- Displaying the logo after suspension or removal
- Implying approval where none exists
- Using the logo to promote non-compliant services
- Reproducing or altering the logo without permission

Sanctions may include:

- Immediate suspension
- Removal from the Code
- Referral to Trading Standards

Post-Exit Obligations

Organisations that leave, are suspended, or are removed from the Code must:

- Immediately cease all use of Code and Scheme branding
- Remove the logo from all materials and websites
- Continue cooperating with ongoing complaints and ADR cases
- Retain relevant records for the required retention period
- Settle any outstanding audit or ADR-related fees

Publication of Enforcement Actions

Transparency

The Code Sponsor may publish:

- Anonymised breach summaries
- Sanctions applied
- Systemic issues identified

Purpose

Publication supports:

- Public confidence
- Deterrence
- Continuous improvement

Reinstatement

Conditions for Reinstatement

Suspended organisations may be reinstated where they:

- Complete required improvement actions
- Demonstrate compliance
- Pass a reinstatement audit

Reinstatement Decision

The Governance Board shall determine reinstatement based on:

- Evidence
- Customer impact
- Assurance of future compliance

Annex F: Glossary of Terms

Purpose

This glossary provides definitions for all terms used in the Code.

Where sector-specific definitions exist (e.g., Ofgem, Ofwat, Ofcom, FCA), the strictest definition applies.

General Definitions

Approved Code Scheme (ACS) The Chartered Trading Standards Institute (CTSI) scheme that approves Codes meeting its Core Criteria and Guidance.

Code Sponsor The organisation responsible for maintaining, publishing, and overseeing compliance with this Code.

Consumer An individual acting wholly or mainly outside the course of business, trade or profession

Cooling-Off Period A 14-day window allowing B2C clients to cancel contracts without penalty.

Governance Board The independent oversight body responsible for monitoring compliance, reviewing sanctions, and approving amendments.

Third Party Intermediary (TPI) Any organisation or individual that advises, procures, negotiates, compares, or switches contracts on behalf of business customers.

Price Comparison Website (PCW) A digital platform that compares products, services, or tariffs and may facilitate switching or procurement.

Vulnerable Consumer Someone who, due to their personal circumstances is especially susceptible to detriment, specific selling techniques or product types and may be less able to represent their own interests, have different needs or be more exposed to behavioural biases.

Code-Specific Definitions

Improvement Plan A structured plan requiring corrective actions following a breach.

Suspension Temporary removal from the Code pending corrective action.

Removal Permanent exclusion from the Code.

Material Change Any change in ownership, structure, or operations that may affect compliance.

Audit A structured review of compliance with this Code.

Thematic Review A review focusing on a specific risk area or practice.

Spot Check An unannounced or short-notice compliance check.

Complaint & ADR Definitions

Complaint Any expression of dissatisfaction requiring a response.

Final Response The organisation's final written position on a complaint, enabling ADR referral.

Alternative Dispute Resolution (ADR) An independent process for resolving disputes outside court, including conciliation and adjudication.

Conciliation An informal ADR stage aimed at reaching mutual agreement.

Adjudication A formal ADR stage where an independent adjudicator issues a binding decision on the organisation.

Binding Decision A decision issued by the ADR body that the organisation must implement.

Data Protection Definitions

Personal Data Any information relating to an identified or identifiable individual.

Business Data Operational or consumption data relating to a business customer.

Data Controller The entity determining the purpose and means of processing personal data.

Data Processor The entity processing data on behalf of a controller.

Data Protection Impact Assessment (DPIA) A documented assessment of risks arising from high-risk data processing.

Data Breach Any security incident leading to loss, alteration, unauthorised access, or disclosure of data.

Energy Sector Definitions

MPAN (Meter Point Administration Number) A unique identifier for electricity supply points.

MPRN (Meter Point Reference Number) A unique identifier for gas supply points.

Half-Hourly (HH) Metering Electricity metering that records consumption every 30 minutes.

Non-Half-Hourly (NHH) Metering Electricity metering that records consumption less frequently.

Pass-Through Charges Industry charges passed directly to customers, including DUoS, TNUoS, and environmental levies.

Erroneous Transfer A switch completed without valid customer consent.

Contracted Capacity The maximum electricity capacity agreed between a customer and the network operator.

Water Sector Definitions

SPID (Supply Point Identifier) A unique identifier for water and wastewater supply points.

Vacancy Status A designation indicating whether a premises is occupied or unoccupied.

Retailer The organisation providing billing and customer service in the business water market.

Wholesaler The organisation responsible for water supply and wastewater removal.

Telecommunications Sector Definitions

CLI (Calling Line Identification) The telephone number presented during a call.

Number Porting The process of transferring a telephone number between providers.

FTTC (Fibre to the Cabinet) Broadband delivered via fibre to the street cabinet and copper to the premises.

FTTP (Fibre to the Premises) Full-fibre broadband delivered directly to the premises.

VoIP (Voice over Internet Protocol) Telephony delivered over internet connections.

Annex G: Version Control

Version	Date	Author	Change Description	Notes
1.0	15/09/2025	Code sponsor	Initial release integrating B2C and B2B standards	Inclusion of sectoral annexes, legal mapping
1.1	15/09/2025	Code sponsor	Added sector specific overlays	Annexes A-D
1.2	15/09/2025	Code sponsor	Integrated legal mapping	Annex E
1.3	15/09/2025	Code sponsor	Defined customer service standards	Annex F
1.4	15/09/2025	Code sponsor	Outlined compliance monitoring and audit mechanism	Annex G

1.5	21/09/2025	Code sponsor	New principles added and current revised	Principles 1,2,5 6,7 and 8
1.6	21/09/2025	Code sponsor	Sector specific additions	Annex A and B
1.7	24/09/2025	James Walker	Code review	Overall review of the code.
1.8	06/10/2025	Code Sponsor	Suggested amendments from internal review	Minor typographical
1.9	13/10/2025	Code Sponsor	Further amendments	Minor grammatical
1.10	08/12/2025	Code Sponsor	Modified to Consumer Switching Code	Significant change to reflect comments of CTSI/ACS
1.11	09/01/2026	Code	Modified to reflect further	Significant change

		Sponsor	comments of CTSI/ACS. Structural modification made to maintain consistency with B2B Code	