Consumer Consent Service Arrangements

Contents

SCHEDULE XX

Consumer Consent Service Arrangements

Version: 0.1 Effective Date: TBC

Domestic Suppliers	Mandatory for Electricity Suppliers for the purposes of sharing Consumer Specific Tariff Information in accordance with the Tariff Interoperability Arrangements Schedule.
Non-Domestic Suppliers	Mandatory for Electricity Suppliers for Relevant TI Non-Domestic Premises
Gas Transporters	N/A
Distribution Network Operators	N/A
DCC	N/A
Metering Equipment Managers	N/A
Non-Party REC Service Users	Mandatory for CCS Users

Change History

Version Number	Implementation Date	Reason for Change
v0.1	N/A	Initial draft for CCS industry consultation

Definitions – to be moved to Schedule 1

The table below sets out additional definitions that are proposed to be added to REC Schedule 1: Interpretations and Definitions. These will supplement the existing definitions used in the REC. Schedule 1 can be found on the REC Portal.

Term	Acronym	Definition
Access Token		means the token issued by the CCS, containing information relating to the Permission granted by the relevant Energy Data Subject, and used by an Authorised Third Party to request data from an Energy Data Holder in accordance with the CCS Arrangements Schedule.
Account Holder		means, for each Registrable Measurement Point, the person or persons identified by the Registered Energy Supplier as the bill payer for that Registrable Measurement Point.
Account Specific Tariff Information Go-Live Date	ASTI Go Live Date	means the go-live date of the provisions of the CCS Arrangements Schedule which apply in relation to RTI Users and/or Account Specific Tariff Information, as per paragraph 1.4 of the CCS Arrangements Schedule.
Authorised Third Party	ATP	means a person that has been (and remains) accredited under paragraph 3 of the CCS Arrangements Schedule to access and use data (subject to obtaining the Permission of the Consumer).
Breaking Change		means a change relating to the CCS API Technical Specification, Data Specification or Permission Purpose Catalogue that requires one or more CCS Users to modify existing Systems, integrations, operational processes or implementations in order to remain compliant.
CCS Account Holder Verification		means the process for verifying that an individual is the person or entity recorded as the Energy Supplier Account Holder.

CCS Address Verification		means the method for verifying that an individual or organisation is the Occupant for a certain address and therefore the appropriate individual or organisation to provide Permission in relation to Metered Data for a specific Registrable Measurement Point.
CCS Administration Portal		means the secure online interface through which RECCo can view and manage CCS User information, enabling updates to be made to the information held in the CCS Directory.
CCS Authorisation Server		means one of the functional components of the CCS, that is responsible for issuing Access Tokens reflecting an Energy Data Subject's Permission and facilitating the sharing of Energy Data.
CCS Consumer Experience Guidelines	CEG	means the Category 3 Product of that name which describes the CCS Permission journeys and the associated user experience guidelines.
CCS Consumer Portal		means the secure online interface through which Energy Data Subjects can grant Permission, view details of organisations which have access to Energy Data and renew or revoke Permissions.
CCS Directory		means one of the functional components of the CCS, holding details of Qualified CCS Users (both Authorised Third Parties and Energy Data Holders) and Data Products available from each individual Energy Data Holder, with the associated metadata.
CCS Error Resolution Paths		means the Category 3 document of that name setting out the approach for resolving errors identified during the execution of operational processes defined in the CCS Arrangements Schedule.

CCS Event Notifications		means a notification provided to a CCS User in accordance with paragraph 14 of the CCS Arrangements Schedule.
CCS Identity Verification	CCS IDV	means the method of verifying that an individual is who they claim to be, as set out in paragraph 12 of the CCS Arrangements Schedule.
CCS Identity Verification Provider	CCS IDVP	means the REC Service Provider responsible for verifying that the individual is the appropriate person to provide Permission to share Energy Data in relation to a specific Premises.
CCS Logo		means the logo approved by RECCo for use by CCS Users in accordance with the CCS Arrangements Schedule, as published by RECCo from time to time.
CCS RMP Matching		means the method for matching a verified address to one or more RMPs, as set out in paragraph 12 of the CCS Arrangements Schedule.
CCS Service Definition		means the document of that name forming part of the Technical Specification that describes the service being provided by the Consumer Consent Service.
CCS Shared Signals Framework		means the mechanism for CCS Users to receive CCS Event Notifications as described in the CCS Arrangements Schedule and CCS Service Definition.
CCS Testing		means the testing required under paragraph 6 of the CCS Arrangements Schedule in order to become a CCS User.
CCS User Portal		means the secure online interface through which CCS Users can view and manage organisational information, enabling updates to be made to the information held in the CCS Directory.

CCS Trade Mark		means the UK trade mark in respect of the CCS Logo with registration number [xxxxx].
Connect API		means the API through which CCS Users may access detailed directory and governance information relating to CCS Users and their associated technical assets.
Consumer Consent API Technical Specification		means the Category 2 Product of that name that describes the specification for Consumer Consent APIs.
Consumer Consent Service Application Programming Interface (API)	CCS API	means the application programming interface used by CCS Users for sending and receiving Consumer Consent Market Messages and the application programming interface used by TI Users to access the TI Supplier Register.
Consumer Consent Service Arrangements	CCS Arrangements	means the arrangements described in the CCS Arrangements Schedule to facilitate the management of Permissions.
Consumer Consent Service Arrangements Schedule	CCS Arrangements Schedule	means REC Schedule [xx].
Consumer Consent Service Market Messages	CCS Market Message	means the Market Messages used to exchange data with the Consumer Consent Service, as defined within the Data Specification. For the purpose of this definition and the exchange of Market Messages, a CCS User shall be treated as if it is a Market Participant.
Consumer Consent Service	CCS	means the service provided pursuant to the CCS Arrangements Schedule and the CCS Service Definition.

Consumer Consent Service Provider	CCS Provider	means the service provider of the Consumer Consent Service.
Consumer Consent Service User	CCS User	means a person that has Qualified (and remains Qualified) as an Authorised Third Party and/or an Energy Data Holder.
Data Product		means a structured reusable package of data that serves a specific purpose or value for users.
Energy Data		means (a) Account Specific Tariff Data; (b) Metered Data; or (c) any other data specified as being in scope of a Data Product approved for inclusion in the CCS in accordance with the CCS Arrangements Schedule.
Energy Data Holder	EDH	means a person that has been (and remains) accredited under paragraph 4 of the CCS Arrangements Schedule to hold and/or process Energy Data.
Energy Data Subject		means (a) for Account Specific Tariff Information, the Account Holder; or (b) for Metered Data, the Occupant.
ID Token		means a token issued in accordance with the CCS API Technical Specification that contains identity information relating to a verified Energy Data Subject.
Mutual Transport Layer Security	mTLS	means a security mechanism where both the client and server authenticate each other, creating a strongly verified, encrypted communication channel.
Non-Breaking Change		means a change relating to the CCS API Technical Specification, Data Specification or Permission Purpose Catalogue that does not require any CCS User to modify existing Systems, integrations, operational processes or implementations in order to remain compliant with the CCS Arrangement.

Occupant		means any person living at or otherwise occupying a Premises who utilises energy supplied to that Premises.
Participants API		means the API through which CCS Users may access information identifying the participants registered within the CCS Directory.
Permission		means the entitlement granted by an Energy Data Subject to an Authorised Third Party to access and use specific Energy Data for one or more defined purposes, in accordance with the requirements of the applicable Energy Code, Energy Licence or other applicable governance arrangements. A Permission may be subject to conditions, including limitations relating to duration, scope or use.
Permission Purpose		means the business purpose for which Permission is granted by an Energy Data Subject to permit an Authorised Third Party to access specified Energy Data.
Permission Purpose Catalogue		means the Category 3 Product maintained by RECCo which specifies the valid set of Permission Purposes that may be used within the Consumer Consent Service.
Permission Purpose Change Process		means the Category 3 Product maintained by RECCo describing the operational arrangements for requesting, assessing, approving, publishing and implementing changes to the Permission Purpose Catalogue.
Refresh Token		means the token issued by the CCS, containing information relating to the Permission granted by the relevant Energy Data Subject, and used to request additional Access Tokens within the overall lifetime of the Permission in accordance with the CCS Arrangements Schedule.

Security Event Token	SET	means the token issued by the CCS, or the TI Energy Supplier in the case of TI Event Notifications, to inform the recipient of an event, in accordance with the CCS Arrangements Schedule and TI Arrangements Schedule.

1. Introduction

1.1 This REC Schedule defines the Consumer Consent Service (CCS) Arrangements, which involve the mechanism for:

(a) verification of individuals through CCS Identity Verification (CCS IDV) or CCS Account Holder Verification;

(b) matching a verified individual to an address through CCS Address Verification and identifying the specific Registrable Measurement Point (RMP) through CCS RMP Matching, for the purpose of sharing Energy Data relating to a specific RMP;

(c) facilitating the granting, review and revocation of Permission to enable the secure sharing of Energy Data between an Energy Data Holder (EDH) and an Authorised Third Party (ATP); and

(d) managing the inclusion of new CCS Users and new Data Products within the CCS Directory.

1.2 This REC Schedule also defines the process by which persons can become CCS Users and the requirements (including assurance activities) applicable to CCS Users to mitigate the risk of data breach and negative Consumer outcomes.

1.3 This REC Schedule should be read in conjunction with:

(a) the CCS Service Definition which defines the service being delivered by the CCS Provider;

(b) the CCS API Technical Specification, which defines the mechanism for exchanging data with the CCS;

(c) the Data Specification, which defines the Market Messages used to interact with the CCS and the associated Data Items;

(d) the Qualification and Maintenance Schedule, which defines the process for REC Service Users to become Qualified and includes the template Access Agreement to be entered into by Non-Party REC Service Users; and

(e) the CCS Consumer Experience Guidelines (CEGs) which describes the CCS Consumer journeys and the associated user experience guidelines.

Transition

1.4 Other than for the purposes of the development and testing of the Tariff Interoperability Arrangements in accordance with Paragraph 1.5, this REC Schedule shall only apply in relation to RTI Users and/or Account Specific Tariff Information from [xx] November 2027 (or such later date as the Secretary of State may designate), being the Account Specific Tariff Information Go-Live Date (ASTI Go-Live Date).

1.5 Before such ASTI Go-Live Date:

(a) each TI Energy Supplier shall develop a mechanism for managing Permission for sharing Account Specific Tariff Information and completing CCS Account Holder Verification, using the CCS API, compliant with the CCS API Technical Specification; and

(b) each TI Energy Supplier shall carry out CCS Testing in order to be Qualified as a CCS User for the purposes of sharing Account Specific Tariff Information.

2. Provision of CCS

2.1 RECCo may contract with one or more REC Service Providers for provision of the CCS, consistent with the description set out in the CCS Service Definition. Where necessary, RECCo shall exercise its rights under the service provider contract(s) to ensure that the contract(s) remain consistent with the CCS Service Definition.

2.2 RECCo shall ensure that the CCS Provider provides each CCS User with access to the CCS, subject to and in accordance with this REC Schedule and, in the case of each CCS User which is not a Party, its Access Agreement.

2.3 RECCo shall ensure that the CCS Directory clearly reflects the level of Qualification maintained in relation to each CCS User, to ensure that CCS Users are only permitted to access Energy Data which that CCS User is authorised to

access. For example, an ATP that is only Qualified as a Registered Tariff Interoperability User (RTI User), shall only be permitted to access Tariff Data.

2.4 It is acknowledged that Energy Data may be shared under the requirements of other Energy Codes or applicable legal and regulatory frameworks. This Schedule applies only to the use of the CCS and does not replace or modify any obligations arising under those arrangements.

2.5 It is acknowledged that data access may be subject to bilateral data sharing agreements between an ATP and an EDH. Each ATP is responsible for ensuring that it has the required agreement in place with the relevant EDH before requesting Permission to access data.

2.6 RECCo's charges for the provision of access to the CCS are set out in the REC Charging Statement. Different charges may be charged for different categories of CCS User, as described in the REC Charging Statement.

2.7 RECCo gives no representation or warranty as to the accuracy or completeness of the data made available by EDHs. Any issues relating to the provision or accuracy of Energy Data provided by EDHs should be raised with the relevant EDH directly.

2.8 RECCo gives no representation or warranty regarding the use of the data made available to ATPs. Any issues relating to the appropriate use of Energy Data should be raised with the relevant ATP directly and reported to RECCo in accordance with Paragraph 9.10.

3. Becoming a CCS User

3.1 An application to become a CCS User will be initiated in accordance with the Qualification and Maintenance Schedule and shall include:

(a) for an organisation that is not eligible to become a Party to this Code, entry into an Access Agreement;

(b) undergoing an Information Security and Data Protection Assessment, unless excluded where the organisation is only Qualifying as an RTI User;

(c) establishing the required public and private keys to enable secure messaging in accordance with this Paragraph 3;

(d) registering information required under the CCS Shared Signals Framework, to enable receipt of CCS Event Notifications, in accordance with this Paragraph 3; and

(e) completing CCS Testing to demonstrate that Market Messages can be exchanged with the CCS in accordance with Paragraph 6.

3.2 The following eligibility rules apply:

(a) only companies are eligible to Qualify as a CCS User (and no other type of person may Qualify); and

(b) a single legal entity may Qualify as both an ATP and an EDH, and there is no restriction on an ATP being an Affiliate of an EDH (or vice versa).

3.3 Where an applicant has become a Party or signed an Access Agreement and successfully completed the Information Security and Data Protection Assessment, the applicant shall obtain the following digital certificates, to be used for the exchange of Market Messages via the CCS Arrangements:

(a) Transport Layer Security (TLS) Certificates, to secure both ends of the network connection ensuring that Market Messages are transferred through a secure encrypted communication channel; and

(b) Message Signing Certificates for each individual CCS User, used to sign the artefacts which the CCS API Technical Specification requires to be signed.

3.4 These certificates will be digitally signed by the CCS Provider to bind certificate owners with their public keys. Each CCS User (or applicant to become a CCS User) shall provide the CCS Provider with details of a security lead who is responsible for managing security certificates on behalf of their organisation.

3.5 Where a CCS User uses a third-party service provider to manage its interactions with the CCS, the service provider shall operate under the CCS User’s security certificates. The CCS User remains accountable for associated obligations.

3.6 Each applicant to become a CCS User shall follow the process set out in the interface table below, which covers the application process, provision of test security certificates for testing and additionally the provision of production security certificates for enduring use. Each security certificate issued under this Paragraph 3.6 shall be used only in the CCS environment for which it was issued.

Ref	When	Action	From	To	Interface	Means
Initial steps applicable to Non-Party REC Service Users only						
3.6.1	As required.	Submit CCS User application.	Applicant	RECCo	Application form	REC Portal
3.6.2	Following 3.6.1.	Validate application against the below criteria: • the company holds a valid registration within Companies House (or equivalent). • confirm organisation is an active registered entity and Directors / Persons of Significant Control are not disqualified.	RECCo		Internal process	N/A
3.6.3	Following 3.6.2	Initiate CCS User Qualification in accordance with the Qualification and Maintenance Schedule. This includes completion of an Information Security and Data Protection Assessment.	Applicant / RECCo		Not defined	N/A

		REC Party applicants will be required to complete an ISDP as part of their Qualification activities.				
3.6.4	Prior to completing the Qualification process.	Accept terms set out within the Access Agreement.	Applicant		Access Agreement	N/A
To be completed by all CCS User applicants						
3.6.5	Following 3.6.4 for a Non-Party REC Service User or starting at this stage for an applicant which is a Party.	Record details of the potential CCS User within the CCS Directory, via the CCS Administration Portal, and update the applicant via an email to the lead contact.	RECCo	Applicant	Not defined	Email
3.6.6	Following receipt of the notification in 3.6.5.	Create an organisation specific Master Admin User within the CCS User Portal and assign individuals to specific roles, including a security lead for security certificate management.	Applicant		Internal process	CCS User Portal

3.6.7	At any time following 3.6.6.	Submit request for test security certificates. This is managed through the CCS User Portal with the applicant generating private keys and a Certificate Signing Request. The Certificate Signing Request is registered in the CCS User Portal to enable future download as required.	Applicant (security lead)		Internal process	CCS User Portal
3.6.8	Following 3.6.7	Validate Certificate Signing Request, including a check to confirm alignment with the organisation's registration details within the CCS Directory. Where the request passes validation, the certificates will be made accessible via the CCS User Portal.	CCS (registration authority)		Internal process	CCS User Portal

3.6.9	Following receipt of test certificates.	Complete external CCS Testing in accordance with Paragraph 6.	Applicant		Internal process utilising CCS test environment	N/A
3.6.10	Following successful completion of CCS Testing.	RECCo to confirm all other Qualification pre-requisites have been successfully completed and approve the CCS User's Qualification.	RECCo	CCS User	Confirmation of Qualification	Not defined
3.6.11	Following 3.6.10.	Update the CCS Directory with confirmation that the organisation has been Qualified as a CCS User	RECCo		CCS Administration Portal	Not defined
3.6.12	Following successful Qualification as a CCS User, or at any future point where new production certificates are required.	Submit request for production security certificates, using the same approach as set out in 3.6.7. Production security certificates will only be provided where the request is from a Qualified CCS User.	CCS User (security lead)		Internal process	CCS User Portal
3.6.13	Following 3.6.12.	Validate Certificate Signing Request, including a check to confirm alignment with the organisation's registration	CCS (registration authority)		Internal process	CCS User Portal

		details within the CCS Directory. Production security certificates will only be provided where the request is from a Qualified CCS User. Where the request passes validation, the certificates will be made accessible via the CCS User Portal.				

Registration to send and receive CCS Event Notifications

3.7 The CCS Shared Signals Framework is used for sending and receiving CCS Event Notifications in accordance with this REC Schedule and TI Event Notifications in accordance with the TI Arrangements Schedule. CCS Users shall implement functionality (in accordance with the OpenID Shared Signals Framework v1.0) as follows:

(a) Each ATP shall be able to receive and process Permission Revocation Notifications, Permission Query Notifications and Permission Verification Required Notifications and shall not delete or otherwise discontinue its stream while it holds any active Permission. Further details of the operational processes and triggers for the issuance of these notifications are set out in Paragraph 14.

(b) RTI Users who wish to receive TI Event Notifications shall also register to receive these notifications in accordance with the TI Arrangements Schedule.

(c) Each TI Energy Supplier shall be able to receive and process Permission Revocation Notifications and Permission Query Notifications to enable it to verify that a valid Permission is in place before issuing a TI Event Notification. TI Energy Suppliers shall also establish functionality to act as a transmitter, to facilitate the

sending of TI Event Notifications in accordance with the TI Arrangements Schedule and the CCS API Technical Specification.

(d) All other EDHs shall be able to receive and process Permission Revocation Notifications and Permission Query Notifications where they need to confirm Permission is in place at a point where no Access Token is presented to it, for example before scheduled or batch data provision or processing of data reliant on Energy Data Subject Permission. It is the responsibility of each EDH to determine, based on its own processing arrangements, whether receipt of Permission Revocation Notifications is required.

3.8 Under the CCS Shared Signals Framework, notifications shall be delivered directly to CCS Users using a push delivery model.

3.9 The following process shall be used to establish and verify a stream for the receipt of CCS Event Notifications. The process for establishing a stream for the receipt of TI Event Notifications is defined in the TI Arrangements Schedule:

Ref	When	Action	From	To	Interface	Means
3.9.1	As required, following CCS User Qualification.	Request CCS SSF endpoint information.	CCS User	CCS Directory	SSF Transmitter Configuration Request	CCS API
3.9.2	Following 3.9.1.	Provide CCS SSF endpoint information.	CCS Directory	CCS User	SSF Transmitter Configuration Response	CCS API
3.9.3	Following 3.9.2.	Register to set up a stream with CCS to receive CCS Event Notifications.	CCS User	CCS	Get SSF Stream Creation Request	CCS API

3.9.4	Following 3.9.3.	Receive confirmation that CCS stream has been established.	CCS	CCS User	SSF Stream Creation Response	CCS API
3.9.5	Following 3.9.4 and at least once per day and no more than once in a 60 second period thereafter.	Initiate verification event to confirm the CCS stream is live and receive any available CCS Event Notifications.	CCS User	CCS	SSF Verification Request	CCS API
3.9.6	Following 3.9.5.	Acknowledge the request and confirm that the CCS stream is live.	CCS	CCS User	SSF Verification Response	CCS API
3.9.7	Following 3.9.6 where the verification Security Event Token is not received within 5 minutes.	Raise a query with the REC service desk. Where the receiver is an EDH, it shall treat its notification channel as unhealthy and suspend notifications to ATPs under affected Permissions until the channel has been verified successfully.	CCS User	CCS	Not defined	CCS User Portal

4. CCS Directory

4.1 The CCS User Portal allows CCS Users to view and manage their own organisational data which is stored in the CCS Directory.

4.2 The CCS User Portal also allows CCS Users to view Data Products available from each EDH. EDHs may update information relating to their own Data Products via the CCS User Portal.

4.3 Where an EDH is only willing to share particular data with an ATP under a bilateral data sharing agreement between the EDH and the ATP, then the EDH shall ensure the CCS Directory reflects the requirement for a bilateral agreement.

4.4 An EDH may hide information regarding Data Products within the CCS Directory to support development and testing activities. However, information is generally expected to be open and available for public consumption.

4.5 An EDH may only add new Data Products to the CCS Directory where prior agreement has been obtained from RECCo. Each new Data Product will be reviewed to ensure alignment between the data being shared and the existing governance arrangements. The process for agreeing new Data Products is set out in Paragraph 10.

Discovery of CCS User Information

4.6 Each CCS User shall use the Participants API to obtain information regarding CCS participants held in the CCS Directory, in accordance with the CCS API Technical Specification.

4.7 Each CCS User shall obtain further information required to support the routing and validation of CCS Market Messages and associated Energy Data requests from the CCS Directory, via the Connect API in accordance with the CCS API Technical Specification.

5. Suspension or Revocation of CCS User Access

5.1 Each CCS User is subject to Performance Assurance, pursuant to which the REC Performance Assurance Board (REC PAB) may determine that a CCS User's access to the CCS should be suspended or revoked (and, if previously suspended, restored). RECCo shall update the CCS Directory, via the CCS Administration Portal, to reflect such determinations. If a CCS User's access is revoked by the REC PAB, RECCo shall terminate the CCS User's Access Agreement.

5.2 RECCo may suspend a CCS User's access where RECCo determines that the CCS User is in breach of any of its obligations under this REC Schedule or the Access Agreement. RECCo may restore a CCS User's access where previously suspended by RECCo. RECCo shall update the CCS Directory, via the CCS Administration Portal, to reflect such suspensions or restorations.

5.3 Where an Energy Data Subject contacts an ATP during a period of suspension, to revoke Permission directly with the ATP, then the ATP shall inform the Energy Data Subject that revocation can only be executed directly by the Energy Data Subject within the CCS Consumer Portal. The ATP shall retain a record of the contact and where the ATP's CCS access is restored, the ATP shall, within 1 Working Day of its CCS access being restored, notify the CCS of the Energy Data Subject's revocation in accordance with Paragraph 14.7, to ensure that such revocation is enacted.

5.4 Suspension of a CCS User's access does not result in associated Permissions being revoked. However, during the period of suspension, the CCS Provider shall revoke the CCS User's security certificates to ensure that the CCS User is unable to obtain new Access Tokens or rely on existing Access Tokens to access or share Energy Data. Existing Permissions shall remain in place unless and until they are otherwise revoked or terminated in accordance with these CCS Arrangements.

5.5 Where a CCS User's access is revoked, RECCo shall notify the CCS Provider who will revoke the relevant security certificates and ensure all active Permissions held within the CCS are terminated.

Revocation of Security Certificates

5.6 A certificate which has been issued by the CCS Provider shall be treated as valid for its stated purpose until such time as it is revoked in accordance with Paragraph 5.7 or expires in accordance with Paragraph 5.10.

5.7 The CCS Provider shall revoke a CCS User's certificate:

(a) where requested by the CCS User's security lead;

(b) where any information in the certificate is known or suspected to be inaccurate;

(c) on suspected or known compromise of the private keys associated with the certificate;

(d) on suspected or known compromise of the media holding the private keys associated with the certificate;

(e) on instruction from the REC PAB (via RECCo), where the CCS User fails to comply with its obligations under this Code and/or its Access Agreement; or

(f) on instruction from RECCo, where the CCS User ceases to be a CCS User.

5.8 In addition, the CCS Provider may revoke a certificate in its sole discretion, to mitigate the risk of a security breach. Where this occurs, a report will be provided to RECCo within two Working Days. Where certificates are revoked, the CCS Provider shall inform the relevant CCS User.

5.9 Where a CCS User's certificates have been revoked, each CCS User and the CCS Provider shall automatically reject any request or Market Message that relies on those certificates.

5.10 The certificate validity periods are as follows:

(a) TLS Certificates require rotation every 12 months; and

(b) Message Signing Certificates require rotation every 24 months.

5.11 CCS Users shall replace TLS certificates at least one month prior to the end of their validity period to ensure continuity of services. An expiry warning will be issued by the CCS Provider to the CCS User three months, one month and one week before the certificate expiration date.

6. External CCS Testing

6.1 Each applicant shall complete external CCS Testing before being provided with production certificates. RECCo shall develop and maintain a CCS testing procedure document, detailing the external CCS Testing arrangements including, as a minimum, required test scenarios, defect management and test data management.

6.2 External CCS Testing shall be initiated following confirmation from RECCo and provision of the required test security certificates in accordance with the process in Paragraph 3.

6.3 Each applicant shall ensure that the test Systems it plans to use for constructing and exchanging Market Messages with the CCS can detect any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them. If unauthorised software is detected or any attempt to install or execute unauthorised software is detected, the installation or execution of that software shall be prevented; and where any such unauthorised software has been installed or executed, the applicant shall take remedial action.

6.4 The CCS Provider shall make the test environments available and provide test support via the REC service desk between 08:00 and 17:00 on each Working Day. The test environment may be used for testing outside these hours but will be unsupported.

6.5 Following completion of external CCS Testing, the applicant shall provide a test completion report to RECCo. RECCo shall review test evidence and determine whether to approve the test completion report. Successful completion of external CCS Testing shall form part of the overall Qualification process as set out in Paragraph 3.

7. General CCS User Requirements

7.1 Each ATP and EDH needs to Qualify (and remain Qualified) as a CCS User in accordance with Paragraph 3 of this REC Schedule and the Qualification and Maintenance Schedule.

7.2 Each CCS User shall exchange Market Messages with the CCS in accordance with the CCS API Technical Specification and the Data Specification. CCS Users shall reject Market Messages which do not conform to the Data Specification.

7.3 Each CCS User shall:

(a) hold valid Cyber Essentials Plus certification;

(b) ensure that all information submitted in support of a security certificate application is true, accurate and that it holds such rights as necessary to any trade marks or other such information submitted during the application for a security certificate;

(c) review the issued security certificate to confirm the accuracy of the information contained within it before installation and first use;

(d) ensure the System used for generating or obtaining a key pair is sufficiently secure to prevent any loss, disclosure, or unauthorised use of the private key;

(e) keep confidential any passwords, passphrases, PINs, private keys or other personal secrets used in obtaining authenticated access to certificates and CCS facilities until it is securely destroyed or deleted. This does not prevent the CCS User sharing details with third party service providers;

(f) make only true and accurate representations to the CCS Provider as to the information required to determine eligibility for a security certificate and for information contained within the security certificate; and

(g) use the security certificate only for the authorised purposes set out in this REC Schedule and the CCS API Technical Specification.

7.4 Each CCS User agrees that it shall not:

(a) knowingly or recklessly introduce into (or transmit via) the CCS or any CCS User Systems any viruses, trojans, worms, logic bombs or other material that is malicious or technologically harmful;

(b) expose any open redirectors;

(c) attempt to gain unauthorised access to the CCS User Portal, CCS Directory or to any Systems used within the CCS Arrangements;

(d) mask or hide the identity of the CCS User's Systems as it connects to the CCS API; and/or

(e) attack the CCS or any CCS User's Systems via a denial of service attack or a distributed denial of service attack.

7.5 Each CCS User shall meet the following requirements to ensure the secure exchange of data:

(a) apply mTLS in accordance with RFC8705 for all secure communications required to support Permission based sharing of data for interactions defined within this REC Schedule. This includes sharing of Energy Data between EDHs and ATPs where Permission has been granted via the CCS, but excludes interactions with publicly available data accessed via the CCS Directory.

(b) only use CCS Authorisation Server metadata obtained from the discovery document published in accordance with the the CCS API Technical Specification:

(c) cache CCS signing key material obtained from the CCS's published key set for a maximum period of 12 hours and no less than 5 minutes: and

(d) confirm that another CCS User's security certificate is published in the CCS Directory before relying on it, refreshing that view at least every 15 minutes.

7.6 Each CCS User shall meet the following requirements in accordance with the CCS Shared Signals Framework:

(a) validate the Security Event Token associated with a CCS Event Notification independently of transport authentication and reject notifications where validation fails;

(b) where a notification includes an unrecognised event type or Permission, discard the notification without acknowledging it as processed and shall raise a query via the REC service desk;

(c) where a CCS User receives multiple CCS Event Notifications relating to a single Permission, record the latest update based on the event timestamp; and

(d) only acknowledge receipt of a CCS Event Notification once the event has been durably persisted.

7.7 Each CCS User may copy, adapt and create derivative works from the Energy Data where necessary for the purposes of providing services to an Energy Data Subject from which it has Permission. Each CCS User agrees that it shall not access, use or exploit the Energy Data or the CCS Arrangements for any purpose other than that explicitly

agreed through the Permission mechanism, and that it shall otherwise keep the Energy Data confidential and not publish or otherwise disclose it, unless explicitly agreed with the Energy Data Subject.

7.8 Each CCS User must revoke the certificate and report to the CCS Provider (via CCS User Portal) any compromise or suspected compromise of the private keys associated with any of their certificates as soon as it becomes aware of such breach or suspected breach to enable certificates to be revoked.

7.9 Each CCS User shall immediately notify RECCo, if the CCS User knows or suspects any unauthorised or unlawful processing of, loss of, damage to, destruction or corruption of, or misuse of any Energy Data, or of any security breach that could compromise the security or integrity of the Energy Data and/or the CCS.

7.10 Each CCS User shall ensure that it carries out assessments that are designed to identify any vulnerability of its Systems prior to accessing any testing services using such Systems and on at least an annual basis. Where a CCS User detects a material vulnerability that impacts its Systems that are part of the CCS Arrangements, the CCS User shall take reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable. The CCS User shall also promptly notify RECCo and the CCS Provider, of the steps being taken to rectify its cause or mitigate its potential impact on CCS Systems and the timescales for rectification.

7.11 Each CCS User shall appoint one or more individuals as its Operational Contact for the purposes of the CCS Arrangements, to facilitate issue resolution. Each CCS User shall record and maintain the details of its Operational Contact(s) within the CCS Directory and shall promptly update those details following any change.

7.12 A CCS User's breach of this Paragraph 7 or Paragraphs 8 and 9 for ATPs and EDHs respectively, shall constitute an Event of Default for the purposes of Clause 16 of the main body of this Code.

Error Resolution

7.13 Where a CCS Market Message fails validation, the CCS User or the CCS Provider shall issue a rejection message using the relevant error code defined in the CCS API Technical Specification. Where the error code identifies an issue with the structure or content of the original CCS Market Message, the CCS User shall amend and resend the CCS Market Message.

7.14 Where a CCS Market Message is sent to the CCS and the originating CCS User receives a synchronous response indicating HTTP 429 (Too Many Requests) or HTTP 503 (Service Unavailable), the relevant CCS Market Message shall be re-sent in accordance with the retry strategy. The retry strategy requires the CCS User to re-attempt delivery in accordance with any 'retry after' value specified in the response, until the request succeeds or a period of 12 hours has elapsed. Where no 'retry after' value is provided, the CCS User should re-attempt delivery at intervals of 300 seconds until the request is successful or a period of 12 hours has elapsed from the initial submission. If the request has not been successfully delivered within that period, the CCS User shall raise a query with the REC service desk.

7.15 Each CCS User shall monitor error messages received and where a CCS Market Message remains undelivered after the retry strategy set out in Paragraph 7.14 has been exhausted, then the CCS User shall follow the process set out in the CCS Error Resolution Paths document.

Monitoring and Reporting

7.16 To support assurance of a CCS User's compliance with its requirements under the CCS Arrangements, RECCo shall utilise CCS monitoring and reporting data to assess CCS User compliance with the CCS API Technical Specification, the Data Specification and the requirements defined in this REC Schedule.

7.17 Each CCS User shall submit information, on request from RECCo, to support Performance Assurance activities, in accordance with the Performance Assurance Schedule.

7.18 For the avoidance of doubt, monitoring is limited to compliance with the CCS Arrangements and does not measure the accuracy of the Energy Data shared by EDHs.

7.19 CCS monitoring and reporting data shall be made available to RECCo to support Performance Assurance activities. Information may also be shared with the Secretary of State and/or Ofgem where requested.

8. Specific Authorised Third Party Requirements

8.1 Each ATP shall ensure engagement with Energy Data Subjects is delivered in accordance with the ATP requirements set out in Appendix 1. ATPs shall provide confirmation to RECCo that they remain compliant with these requirements on an annual basis.

8.2 In the case of Energy Data that comprises Personal Data, each ATP is responsible for determining the relevant lawful basis on which it is relying for the processing of that Personal Data in accordance with Data Protection Legislation. Nothing in the REC provisions removes this responsibility.

8.3 Notwithstanding Paragraph 8.2, ATPs may be required to obtain Permission via the CCS based on rules set out within this Code or other Energy Codes or Energy Licences which restrict access to Energy Data without Permission being granted via the CCS.

8.4 Each ATP shall ensure that its Systems and processes are compliant with the requirements of the FAPI 2.0 Security Profile applicable to it in its role as a client, including those at clauses 5.2, 5.3.1, 5.3.3 and 5.4. Each ATP shall additionally comply with the requirements applicable to ATPs set out in this Paragraph 8 and the CCS API Technical Specification. Where it is identified that a requirement in this Paragraph 8 or the CCS API Technical Specification applicable to ATPs is not consistent with the FAPI 2.0 Security Profile, RECCo shall progress a Change Proposal to maintain alignment.

8.5 When communicating with the CCS Authorisation Server, each ATP shall obtain the issuer URL from the CCS Directory, using a secure channel, such that it cannot be modified by an attacker. The ATP shall verify that the issuer URL matches the issuer value contained in the CCS Authorisation Server discovery document.

8.6 When requesting Energy Data from an EDH, each ATP shall rely on information about the EDH held within the CCS Directory and obtained via the Connect API.

8.7 Where an ATP requires Permission via the CCS to access Energy Data, the ATP shall ensure that the Energy Data Subject has provided agreement before an authorisation request is initiated. Authorisation requests shall be protected against cross-site request forgery and other unauthorised initiation mechanisms, ensuring that the Energy Data Subject is aware of the ATP requesting access and the context in which the authorisation process was initiated.

8.8 Each ATP shall specify within the authorisation request: (a) the type of Energy Data required (b) the purpose(s) for which the Energy Data will be used, (c) the period for which Permission is required; and (d), where applicable, the period to which the requested Energy Data relates. The ATP shall ensure that the information included in its authorisation request matches the information made available to the Energy Data Subject at the point Permission is obtained. The ATP shall only ask for the minimum access and Energy Data that is genuinely needed to provide the service.

8.9 When specifying the purpose(s) for which the Energy Data will be used, the ATP shall ensure that each purpose aligns with one of the Permission Purposes recorded within the current version of the Permission Purpose Catalogue. Additional Permission Purposes can be added in accordance with the process in Paragraph 11.

8.10 Each ATP may provide an Energy Data Subject address as part of the initial authorisation request. The CCS-verified address obtained via CCS Address Verification shall be used for Occupancy validation and determining the RMPs associated with a Permission, with ATP-supplied addresses treated as indicative information only. Each ATP remains responsible for validating that the CCS-returned address is suitable for their service and compliant with their Data Protection Legislation obligations. Where a mismatch is identified, each ATP shall assess whether their service can continue and revoke Permission if the address is not appropriate for the intended use.

8.11 Where the ATP has obtained an evergreen Permission from the Energy Data Subject, the ATP shall set the expiry date within its authorisation request at a maximum of three years after the date that Permission was obtained. After this time, the ATP shall initiate a new authorisation request if data access is still required.

8.12 Where the ATP has obtained one-time Permission for access to Energy Data, the ATP shall initiate revocation of that Permission immediately after the Permission has been exercised, in accordance with the process set out in Paragraph 14.7. For one-time Permission, the ATP shall not provide an expiry date as the CCS will set the expiry date to 25 hours after the Permission start date, to accommodate scenarios where the relevant Energy Data is not available within a shorter timeframe. A one-time Permission is not exercised until the requested Energy Data has been received in full, including any Energy Data provided asynchronously by an EDH.

8.13 Each ATP shall retain details of the Grant Id and Permission Expiry Date provided by the CCS and use this when issuing a revocation notification to the CCS in accordance with the process in Paragraph 14.7. ATPs shall not rely on the Grant Id as a means of identifying the Energy Data Subject within their own Systems and processes.

8.14 Each ATP shall carry out regular (at least quarterly) reconciliation of Permission data between its own records and records held by the CCS using the grant status capability defined in the CCS API Technical Specification. Where discrepancies are identified, the ATP shall investigate and update records accordingly.

8.15 The ATP shall not use the Energy Data for any purpose other than the purpose specified in the authorisation request and subsequently recorded by the CCS against the Permission associated with that Grant Id.

8.16 Where the ATP identifies that the individual who granted Permission in relation to the specific Energy Data is no longer the appropriate individual, for example where the Energy Data Subject moves out of the associated Premises, the ATP shall treat the Permission as being revoked and notify the CCS within 1 Working Day, in accordance with Paragraph 14.7.

8.17 Each ATP shall ensure that it has procedures in place to investigate and act upon a Permission Verification Required Notification received from the CCS relating to a potential change in an Energy Data Subject's circumstance.

8.18 Each ATP shall ensure that there is an easily accessible mechanism in place to allow the Energy Data Subject to revoke their Permission. Where Permission is revoked by the Energy Data Subject, the ATP shall issue a revocation notification to the CCS within 1 Working Day in accordance with Paragraph 14.7.

8.19 Each ATP shall ensure that it has policies and procedures in place to manage Energy Data Subject queries and complaints regarding the CCS Arrangements, including the ability to provide details of active Permission on request by the Energy Data Subject.

8.20 Where a query is raised by an Energy Data Subject in accordance with Paragraph 14.4, the ATP shall investigate the query and provide a response within 5 Working Days.

9. Specific Energy Data Holder Requirements

9.1 Each EDH shall determine, in accordance with the applicable Energy Code or Energy Licence, whether a request for Energy Data is one for which Permission via the CCS is required before releasing the requested Energy Data to an ATP. The requirement for Permission via the CCS may apply irrespective of the lawful basis relied upon by the ATP under Data Protection Legislation.

9.2 Each EDH shall ensure that its Systems and processes are compliant with the requirements of the FAPI 2.0 Security Profile applicable to it in its role as a resource server, including those at clauses 5.2, 5.3.1, 5.3.4 and 5.4. Each EDH shall additionally comply with the requirements applicable to EDHs set out in this Paragraph 9 and the CCS API Technical Specification. Where it is identified that a requirement in this Paragraph 9 or the CCS API Technical Specification applicable to EDHs is not consistent with the FAPI 2.0 Security Profile, RECCo shall progress a Change Proposal to maintain alignment.

9.3 Each EDH shall validate the Access Token in accordance with clause 5.3.4 of the FAPI 2.0 Security Profile and the requirements applicable to EDHs in the CCS API Technical Specification, including verifying its integrity and expiry, that the security certificate presented by the ATP corresponds to the ATP identified in the Access Token, and that the data request relates only to the Energy Data and data period authorised by the Access Token.

9.4 Where an Access Token is invalid, expired, revoked or does not authorise the requested access to Energy Data, the EDH shall reject the request and return an appropriate error response.

9.5 Each EDH shall ensure that the Energy Data issued to an ATP is consistent with the scope of the Permission defined in the Access Token.

9.6 Where Permission includes future data processing and / or data sharing triggered by the EDH, for example through an internal event or scheduled activity, the EDH shall record the Grant Id and Permission Expiry Date relating to the Permission and shall monitor Permission Revocation Notifications and Permission Query Notifications. The EDH shall not commence or continue any activity under a Permission once either of these notifications has been received.

9.7 Where an EDH is required to monitor Permission Revocation Notifications and Permission Query Notifications under Paragraph 3.7, it shall not send notifications or Energy Data to an ATP under a Permission while its CCS notification channel is unverified, unhealthy or paused, and shall suspend rather than abandon such notifications until the channel has been verified successfully. An EDH shall not hold its own record of the Permission, nor treat any record it holds as authority to serve data, since serving data always requires a valid Access Token presented on the request.

9.8 Where an EDH receives a request for one-time access, it shall record the Grant Id and shall refuse any subsequent retrieval request using the same Grant Id once the data has been delivered in full. Where delivery of the data requires more than one call, for example where a retrieval call follows a notification, all calls required to complete that delivery shall collectively be regarded as a single retrieval.

9.9 Each EDH shall maintain details of available Data Products within the CCS Directory, including the relevant endpoints. EDHs shall highlight where bilateral arrangements are required before an ATP can access Energy Data relating to a specific Data Product and shall provide sufficient information to enable ATPs to identify any additional steps required before issuing a data request.

9.10 Each EDH shall immediately notify RECCo if it becomes aware of, or suspect:

(a) an ATP has suffered a security breach that could compromise the security, confidentiality or integrity of the Energy Data and/or the CCS; or

(b) where an ATP is, or may be, failing to comply with any provision of this REC Schedule or is otherwise acting in a manner that could adversely affect the security, integrity or proper operation of the CCS Arrangements.

9.11 Each EDH shall provide a mechanism to enable queries regarding the sharing of Energy Data to be raised by ATPs.

10. Addition of new Data Products

10.1 Where an EDH wishes to introduce a new Data Product into the CCS Directory, the EDH shall ensure that the proposed Data Product is assessed to determine whether the existing CCS governance arrangements adequately protect the data being shared.

10.2 Therefore, before adding a new Data Product, the EDH shall complete the CCS Data Product Proforma for RECCo review. A key purpose of the CCS Data Product Proforma shall be to enable RECCo to assess whether the Data Product permits the sharing of a new type of data that is not already addressed by the existing CCS governance arrangements.

10.3 On receipt of a CCS Data Product Proforma, RECCo shall review the proposal and consider the following elements:

(a) Legal basis – whether the EDH has the relevant legal basis for holding and / or accessing the data and sharing it with ATPs. This may include a review of the EDH's Data Protection Impact Assessment or equivalent evidence;

(b) Scope – whether the data being shared is appropriate for inclusion within the CCS, for example is it Consumer owned data requiring Permission from the Consumer;

(c) Terms – the contractual terms governing the relationship between the EDH and the ATP, including requirements on ATPs in relation to downstream sharing of data;

(d) Accreditation – whether there are any additional Qualification or verification steps an ATP is required to complete to obtain the new data set;

(e) Data retention – the arrangements in place for the retention and deletion of data once consent expires or the purpose for processing the data has been fulfilled;

(f) CCS IDV – the confidence level associated with the Data Product in accordance with Good Practice Guide (GPG) 45;

(g) CEG impacts – whether the new Data Product requires amendments to the CEGs, for example, if the new Data Product expands the scope into a new type of data which may need bespoke guidance; and

(h) Data Source – whether a single organisation is providing a bespoke data set or multiple organisations are providing access to a standardised set of data, for example all Energy Suppliers providing access to Consumer contact details in a standard format.

10.4 Where RECCo considers that the new Data Product can be included without a change to the CCS governance model, RECCo shall approve the Data Product for inclusion in the CCS Directory.

10.5 Where RECCo determines that amendments to the CCS governance arrangement are required before a new Data Product can be included in the CCS Directory, RECCo shall engage with the EDH to agree the required changes and progress a REC Change Proposal.

11. Governance of Permission Purposes

11.1 RECCo shall establish, maintain and publish the following Category 3 Products for the purposes of supporting the operation of the CCS:

(a) the Permission Purpose Catalogue; and

(b) the Permission Purpose Change Process.

11.2 The Permission Purpose Catalogue shall define the valid Permission Purpose enumerations that may be used within the Permission Purpose Data Item specified within the Data Specification.

11.3 Where the Data Specification refers to the Permission Purpose Data Item, the valid values for that Data Item shall be the values published in the current version of the Permission Purpose Catalogue.

11.4 RECCo shall maintain the Permission Purpose Catalogue in accordance with the Permission Purpose Change Process and shall:

(a) publish the current version of the Permission Purpose Catalogue on the REC Portal;

(b) maintain a version history of the Permission Purpose Catalogue;

(c) publish the implementation date for each approved change;

(d) publish each determination made under the Permission Purpose Change Process, together with the supporting rationale; and

(e) make previous versions of the Permission Purpose Catalogue available for reference.

11.5 RECCo shall determine, in accordance with the Permission Purpose Change Process, whether a proposed amendment to the Permission Purpose Catalogue constitutes a Non-Breaking Change.

11.6 Where RECCo determines that a proposed amendment to the Permission Purpose Catalogue constitutes a Non-Breaking Change, RECCo shall approve or reject the proposal in accordance with the Permission Purpose Change Process.

11.7 Where RECCo determines that a proposed amendment to the Permission Purpose Catalogue does not constitute a Non-Breaking Change, that amendment shall only be progressed through the REC Modification Process in accordance with Schedule 5.

11.8 RECCo shall publish and maintain the Permission Purpose Change Process, which shall set out the operational arrangements for:

(a) submitting requests for amendments to the Permission Purpose Catalogue;

(b) assessing proposed amendments, including the criteria for determining whether a proposed amendment constitutes a Non-Breaking Change;

(c) consultation and stakeholder engagement, where appropriate;

(d) decision-making;

(e) publication of determinations;

(f) implementation and version management; and

(g) such other operational arrangements as RECCo reasonably considers necessary for the effective management of the Permission Purpose Catalogue.

11.9 Where an ATP wishes to introduce a new Permission Purpose into the Permission Purpose Catalogue, it shall submit a request in accordance with the Permission Purpose Change Process.

12. Use of the CCS Logo

12.1 RECCo shall publish the CCS Logo and make it available to CCS Users, together with any applicable brand guidelines, on the REC Portal or such other location as RECCo may determine.

12.2 Each organisation that is Qualified under this REC Schedule as a CCS User is hereby granted a royalty-free, non-exclusive, non-transferable licence to use the CCS Logo in the United Kingdom for the period of its Qualification as further described in this Paragraph 12.

12.3 Each CCS User shall:

(a) comply with any and all brand guidelines concerning the use of the CCS Logo as may be issued and updated by RECCo from time to time;

(b) not use the CCS Logo or any Conflicting Brand in any way which damages (or which may damage) RECCo, the CCS, the CCS Logo or the reputation or goodwill attaching to any of them;

(c) promptly notify RECCo if the CCS User becomes aware of any unauthorised use of, or any infringement of any intellectual property in, the CCS Logo or CCS Trade Mark (or any claims or actions in connection with the CCS Logo or CCS Trade Mark); and

(d) not use the CCS Logo or any Conflicting Brand in any manner which RECCo reasonably considers to be misleading.

12.4 The REC PAB may determine that a CCS User's licence to use the CCS Logo is to be suspended or withdrawn where that person does not comply with Paragraph 12.3. For the avoidance of doubt, a failure to comply with Paragraph 12.3 may also be treated as an Event of Default under Clause 16 (Events of Default and Consequences of Default) of the Main Body of this Code.

12.5 Any CCS User whose Qualification has been suspended or withdrawn in accordance with this REC Schedule shall immediately cease to use and desist from using the CCS Logo and/or any Conflicting Brand.

12.6 The CCS Trade Mark belongs to RECCo. The general licence in Clause 13.4 (REC Materials) of the Main Body of this Code shall not apply to the CCS Logo. No Party other than RECCo shall attempt to register as a trade mark, or otherwise claim rights in the CCS Logo or any Conflicting Brand, in any part of the world.

13. CCS Identity Verification

13.1 The CCS IDV arrangements seek to verify that the individual granting Permission for access to Energy Data is an appropriate Energy Data Subject. The determination of who the correct individual is, will be based on the type of Energy Data being accessed:

(a) where the ATP is seeking to access Metered Data, the individual providing Permission shall be the Occupant at the relevant Premises. In this scenario the CCS Identity Verification Provider (IDVP) will verify that the individual is a valid Occupant for the address in question; and

(b) where the ATP is seeking to access Account Specific Tariff Information, the individual providing Permission shall be the Account Holder. In this scenario the Registered Energy Supplier will verify that the individual is the valid Account Holder.

CCS Address Verification and CCS RMP Matching

13.2 To support requests for access to Metered Data, RECCo shall implement and manage CCS IDV services from one or more CCS IDVPs, to deliver CCS IDV and CCS Address Verification. The level of verification completed as part of

the CCS IDV process shall be sufficiently flexible to reflect the type of Energy Data being accessed and the purpose of data access.

13.3 Following successful CCS IDV and CCS Address Verification undertaken as part of a request for access to Metered Data, the CCS IDVP shall provide confirmation to the CCS that the individual is the Occupant, together with the address of the Premises in question.

13.4 Following initial CCS Address Verification, an Energy Data Subject shall be required to re-verify that they are the Occupant at least every three years.

13.5 On receipt of the verified individual's details, the CCS shall identify the RMP(s) at the Premises using data from the Gas Enquiry Service and / or Electricity Enquiry Service and include this information in the Access Token issued to the relevant ATP. To support this matching activity, RECCo shall retain a record of Retail Energy Location (REL) Address Data associated with each RMP, alongside other information to support identification of the RMP relevant to the specific Permission request.

13.6 Where the CCS IDV validates that the individual is the current Occupant but is unable to validate occupancy for the full requested period, the CCS shall restrict the data period authorised in the Access Token so that it does not begin before the start of the occupancy period validated by the IDV Provider.

CCS Account Holder Verification

13.7 To support requests for access to Account Specific Tariff Information, each Registered Energy Supplier shall implement a process to confirm that an individual is the Account Holder and shall provide the RMP(s) against which the individual is able to provide Permission in accordance with Paragraph 14.10 and the CCS API Technical Specification.

13.8 Each Energy Supplier that is required to support CCS Account Holder Verification shall apply the OpenIDConnect (OIDC Core 1.0) specification, together with the following CCS specific requirements:

(a) using mutual TLS (mTLS) for secure transport of the identity token;

(b) implementing the private_key_jwt method for authentication of the CCS Authorisation Server; and

(c) requiring the use of signed request objects compliant with the OAuth JWT-Secured Authorisation Request (JAR) standard to ensure the integrity and authenticity of authorisation requests.

14. Operational Processes

14.1 This Paragraph 14 defines the end-to-end processes that form part of the Consumer Consent Arrangements.

Granting Permission for access to Account Specific Tariff Information

14.2 An ATP (RTI User) wishing to access Account Specific Tariff Information shall follow the process set out in the Tariff Interoperability Arrangements Schedule.

Granting Permission for access to Metered Data

14.3 An ATP wishing to access Metered Data shall follow the process in the interface table below. Where Permission is granted, the ATP shall use the Refresh Token provided in relation to an individual Permission to request additional Access Tokens in accordance with the operational steps set out in this interface table until the Permission expires or is revoked. For one-time Permission, the ATP shall revoke the Refresh Token in accordance with Paragraph 8.12 once the Permission has been exercised.

Ref	When	Action	From	To	Interface	Means
14.3.1	As required.	Engage with Occupant to agree services.	ATP	Occupant	Not defined	N/A
14.3.2	Where the ATP determines that Permission is required in order to access Energy Data.	Submit authorisation request.	ATP	CCS	Pushed Authorization Request	CCS API
14.3.3	Following 14.3.2 where the message passes validation.	Return unique reference for the request (request_uri) which the ATP uses to divert the Occupant to the CCS.	CCS	ATP	Pushed Authorization Request Response	CCS API

14.3.4	Following 14.3.3	Occupant provides email address to allow CCS to determine whether they have a CCS account. Where the Occupant has a CCS account, progress to 14.3.5. Where the Occupant does not have a CCS account, progress to 14.3.6.	Occupant	CCS	Not defined	CCS Consumer Portal
14.3.5	Following 14.3.4, where the Occupant has a CCS account.	Log into CCS account and confirm address has not changed. Where address has changed, progress to 14.3.7. Where address has not changed, progress to 14.3.11.	Occupant	CCS	Not defined	CCS Consumer Portal
14.3.6	Following 14.3.4, where the Occupant does not have a CCS account.	Validate email address using One Time Password and establish a CCS account.	Occupant	CCS	Not defined	CCS Consumer Portal
14.3.7	Following 14.3.4 or 14.3.6 where CCS IDV is required.	Occupant is invited to complete CCS IDV. Where CCS IDV is not successful, progress to 14.3.8. Where CCS IDV is successful, progress to 14.3.10.	Occupant	CCS IDVP	Not defined	CCS Consumer Portal
14.3.8	Following 14.3.7, where the CCS IDVP is unable to confirm the Occupant's address.	Provide notification that the CCS IDV process has failed.	CCS IDVP	CCS	Internal process	CCS API

14.3.9	Following 14.3.7 where CCS IDV has failed.	Provide notification that the CCS IDV process has failed in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A
14.3.10	Following 14.3.7, where the CCS IDVP confirms the Occupant's address.	Provide confirmation of successful CCS IDV, including the verified address.	CCS IDVP	CCS	Internal process	CCS API
14.3.11	Following 14.3.10.	Match the Occupant to one or more RMPs using data from the Enquiry Services. Where CCS RMP Matching is unsuccessful, progress to 14.3.12. Where RMP Matching is successful, progress to 14.3.13.	CCS		Internal process	N/A
14.3.12	Following 14.3.11, where the CCS is unable to confirm the RMP(s) for the verified address.	Provide notification that the RMP Matching process has failed in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A
14.3.13	Following 14.3.11 where the Occupant has passed the CCS IDV checks and been matched to a specific RMP or following 14.3.5 where a returning Occupant has confirmed their	Request Occupant to confirm that they are the Occupant and whether they wish to provide Permission for the Energy Data to be shared. Where the Occupant does not provide Permission, progress to 14.3.14. Where the Occupant does provide Permission, progress to 14.3.15.	CCS	Occupant	Not defined	CCS Consumer Portal

	address has not changed.					
14.3.14	Following 14.3.13 where the Occupant does not provide Permission.	Notify ATP of failed Permission journey in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A
14.3.15	Following 14.3.13. where the Occupant grants Permission for the ATP to access their Metered Data.	Record Permission against specific RMP and ATP and provide authorization code. At this stage the Occupant is re-directed back to the ATP in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A
14.3.16	Following 14.3.15	Create permission record and store Grant Id and Expiry Date. Use the authorization code via a secure channel to request Refresh Token and Access Token.	ATP	CCS	Token Request	CCS API
14.3.17	Following 14.3.16 where the message passes validation.	Provide Refresh Token to enable future Access Tokens to be requested during the period of Permission and an Access Token for the immediate request.	CCS	ATP	Token Response	CCS API
14.3.18	Following receipt of a valid Access Token.	Use Access Token provided by the CCS to request access to the required Energy Data.	ATP	EDH	EDH specific API including CCS authorisation header	EDH defined API
14.3.19	Following 14.3.18.	Validate Access Token, in accordance with the CCS API Technical Specification, to confirm whether appropriate Permission is in place. Where	EDH		Internal process	N/A

		the Permission does not reflect one-time access, the EDH shall store the Grant Id and Expiry Date. Where Permission is not in place, progress to 14.3.20. Where Permission is in place, progress to 14.3.21.				
14.3.20	Following 14.3.19 where Permissions is not in place.	Reject the request for Energy Data.	EDH	ATP	EDH defined error codes	EDH defined API
14.3.21	Following 14.3.19, where Permission is in place.	Provide Energy Data.	EDH	ATP	EDH defined API	EDH defined API
14.3.22	Following 14.3.21.	Energy Data used solely for the provision of the agreed service to the Occupant and in accordance with the applicable Permission Purpose.	ATP	Occupant	Not defined	N/A

Energy Data Subject Permission Management

14.4 Where an Energy Data Subject has established a CCS account and granted Permission to an ATP through the CCS, the Energy Data Subject can view, query or revoke Permission in accordance with the interface table below:

Ref	When	Action	From	To	Interface	Means
Viewing Existing Permissions						
14.4.1	As required	Energy Data Subject logs into CCS account to view existing Permission. Where the Energy Data Subject identifies a Permission they do not recognise or otherwise wish to terminate	Energy Data Subject		Internal process	CCS Consumer Portal

		access to Energy Data, the next steps will depend on who granted the original Permission. Where the relevant Energy Data Subject granted the original Permission, proceed to 14.4.2. Where the relevant Energy Data Subject did not grant the original Permission, proceed to 14.4.7.				
Permission Revocation						
14.4.2	Following 14.4.1, where the Energy Data Subject wishes to revoke Permission.	Initiate Permission revocation.	Energy Data Subject		Not defined	CCS Consumer Portal
14.4.3	Following 14.4.2.	Update Permission record and issue Permission Revocation Notification.	CCS	ATP	Permission Revocation Notification	CCS API
14.4.4	Following 14.4.3.	Update records to reflect revocation of Permission.	ATP		Internal process	N/A
14.4.5	In parallel with 14.4.3, where the EDH has registered to receive Permission Revocation Notifications.	Issue Permission Revocation Notification.	CCS	EDH	Permission Revocation Notification	CCS API
14.4.6	Following 14.4.5.	Update Systems to prevent further sharing of Energy Data, or in the case of TI Energy Supplier, further sharing of TI Event Notifications.	EDH		Internal process	N/A

Permission Query						
14.4.7	Following 14.4.1, where the Energy Data Subject wishes to query Permission.	Initiate Permission query process.	Energy Data Subject		Not defined	CCS Consumer Portal
14.4.8	Following 14.4.7.	Log query against Permission record, terminate Permission and issue Permission Query Notification.	CCS	ATP	Permission Query Notification	CCS API
14.4.9	Following 14.4.8.	Contact the original Energy Data Subject and seek to resolve the query. Where the ATP believes that there has been an issue with the CCS IDV or RMP Matching process proceed to 14.4.10. Otherwise, proceed to 14.4.11.	ATP		Internal process	N/A
14.4.10	Following 14.4.9	Raise a service desk query via the REC Portal and progress in accordance with the CCS Error Resolution Paths document.	ATP	CCS	Not defined	REC Portal
14.4.11	Following 14.4.9 and within 5 Working Days of the original query being raised.	Complete the investigation and resolve query within the CCS User Portal.	ATP	CCS	Not defined	CCS User Portal
14.4.12	Following 14.4.11	Update CCS Consumer Portal information to confirm to Energy Data Subject that the Permission query has been concluded.	CCS	Energy Data Subject	Not defined	CCS Consumer Portal
14.4.13	Following 14.4.12,	Following completion of the Permission query investigation, where the ATP	ATP		Internal process	N/A

		wishes to continue accessing Energy Data, a new Permission must be granted through the CCS in accordance with the process in Paragraph 14.3.				
14.4.14	Following 14.4.7, where the EDH has registered to receive CCS Event Notifications.	Issue Permission Query Notification.	CCS	EDH	Permission Query Notification	CCS API
14.4.15	Following 14.4.14.	Update Systems to prevent further sharing of Energy Data, or in the case of TI Energy Supplier, further sharing of TI Event Notifications.	EDH		Internal process	N/A

Energy Data Subject Address Data Management

14.5 Where an Energy Data Subject has established a CCS account and granted Permission to an ATP through the CCS, the Energy Data Subject can view and amend its personal data, in accordance with the interface table below:

Ref	When	Action	From	To	Interface	Means
14.5.1	As required	Energy Data Subject logs into CCS account to view personal data. Where the Energy Data Subject identifies a change of address is required, they may update their data directly.	Energy Data Subject		Internal process	CCS Consumer Portal
14.5.2	Following 14.5.1, where the Energy Data Subject updates their address data and has previously	Address data update triggers CCS IDV. Energy Data Subject is invited to complete CCS IDV to verify Occupancy.	Energy Data Subject		Not defined	CCS IDV

	been subject to CCS Address Verification to verify Occupancy.	Where CCS IDV is not successful, progress to 14.5.3. Where CCS IDV is successful, progress to 14.5.5.				
14.5.3	Following 14.5.2, where the CCS IDVP is unable to confirm Occupancy.	Provide notification that the CCS IDV process has failed.	CCS IDVP	CCS	Internal process	CCS API
14.5.4	Following 14.5.3	Provide notification that the CCS IDV process has failed in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A
14.5.5	Following 14.5.2, where the CCS IDVP confirms Occupancy.	Provide confirmation of successful CCS IDV, including the verified address.	CCS IDVP	CCS	Internal process	CCS API
14.5.6	Following 14.5.5.	Match the Occupant to one or more RMPs using data from the Enquiry Services. Where CCS RMP Matching is not successful, progress to 14.5.7. Where RMP Matching is successful, progress to 14.5.8.	CCS		Internal process	N/A
14.5.7	Following 14.5.6, where the CCS is unable to confirm the RMP(s) for the verified address.	Provide notification that the RMP Matching process has failed in accordance with CCS API Technical Specification.	CCS	ATP	CCS redirection	N/A

14.5.8	Following 14.5.6, where CCS RMP Matching is successful.	Update the verified address and associated RMP(s) recorded within the CCS	CCS		Internal process	N/A
14.5.9	Following 14.5.1.	Revoke all active Permissions associated with the previous RMP(s) and update the CCS Permission Records	CCS		Internal process	N/A
14.5.10	Following 14.5.9.	Notify the relevant ATP(s) that the Permission(s) has been revoked as a result of the address change.	CCS	ATP	Permission Revocation Notification	CCS API
14.5.11	In parallel with 14.5.9, where the EDH has registered to receive Permission Revocation Notifications.	Issue Permission Revocation Notification.	CCS	EDH	Permission Revocation Notification	CCS API
14.5.12	Following 14.5.11	Update Systems to prevent further sharing of Energy Data.	EDH		Internal process	N/A

Energy Data Subject CCS Account Deletion

14.6 An Energy Data Subject may choose to close their CCS account at any time. Closure of a CCS account will result in the withdrawal of all active Permissions associated with that CCS account with Permission Revocation Notifications in accordance with Paragraph 14.4. Following CCS account deletion, the CCS shall retain Energy Data Subject information where required to satisfy legal, regulatory, security, audit and operational obligations.

ATP Led Permission Revocation

14.7 Where an ATP becomes aware that Permission is no longer valid, it shall follow the process in the interface table below:

Ref	When	Action	From	To	Interface	Means
14.7.1	Within 1Working Day of the ATP becoming aware of a requirement to revoke Permission. This may be initiated directly by an Energy Data Subject or may be based on the ATPs own records of occupancy or contract duration.	Initiate Permission revocation.	ATP	CCS	Token Revocation Request	CCS API
14.7.2	Following 14.7.1.	Issue acknowledgment of receipt.	CCS	ATP	Standard HTTP acknowledgement	CCS API
14.7.3	In parallel with 14.7.2.	Process Permission revocation and issue Permission Revocation Notification.	CCS	ATP	Permission Revocation Notification	CCS API
14.7.4	Following 14.7.3.	Update records to reflect revocation of Permission	ATP		Internal process	N/A
14.7.5	In parallel with 14.7.3, where the EDH has registered to receive Permission Revocation Notifications.	Issue Permission Revocation Notification.	CCS	EDH	Permission Revocation Notification	CCS API
14.7.6	Following 14.7.5.	Update Systems to prevent further sharing of Energy Data, or in the case of TI Energy	EDH		Internal process	N/A

		Supplier, further sharing of TI Event Notifications.				
14.7.7	Following 14.7.1, where the revocation reason suggests that the ATP believes the Energy Data Subject is no longer the Occupant for the verified Premises.	Issue Permission Verification Required Notification to other ATPs with active Permission reliant on CCS Address Verification of the associated Occupant.	CCS	ATP	Permission Verification Required Notification	CCS API
14.7.8	Following receipt of the notification in 14.7.7 by each impacted ATP.	Contact the Energy Data Subject to verify that the Permission remains appropriate. Where Permission is no longer appropriate, each ATP should initiate revocation in accordance with this Paragraph 14.7. The ATP shall not treat the Permission Verification Required Notification as a Permission revocation and shall not cease access to data on the basis of the CCS Event Notification alone	ATP	Energy Data Subject	Not defined	N/A

ATP Led Permission Renewal

14.8 Where an ATP becomes aware that Permission is due to expire, it shall follow the process in the interface table below:

Ref	When	Action	From	To	Interface	Means
14.8.1	As required, where the ATP is seeking to extend access to data.	Engage with Energy Data Subject to determine whether to extend access to data.	ATP	Energy Data Subject	Not defined	N/A

14.8.2	Following 14.8.1, where agreed that renewal of Permission is required.	Submit authorisation request with original Grant Id.	ATP	CCS	Pushed Authorization Request	CCS API
14.8.3	Following 14.8.2 where the message passes validation.	Return unique reference for the request (request_uri)	CCS	ATP	Pushed Authorization Request Response	CCS API
14.8.4	Following 14.8.3.	The Energy Data Subject will be redirected to the CCS and asked to renew Permission. CCS IDV will not be required unless the Energy Data Subject confirms they have moved or the previous CCS Address Verification activity was completed more than three years ago. Where CCS Address Verification is required, this will be completed before asking the Energy Data Subject to renew Permission. If the CCS Address Verification fails, the CCS will notify the ATP and terminate the process.	Energy Data Subject		Not defined	N/A
14.8.5	Following 14.8.4, where the Energy Data Subject chooses not to renew Permission.	Notify ATP of failed Permission journey.	CCS	ATP	CCS redirection	N/A
14.8.6	Following 14.8.4, where the Energy Data Subject renews Permission.	Record Permission against specific RMP and ATP and provide authorization code in accordance with the CCS API Technical Specification. At this stage the Occupant is re-directed back to the ATP and the journey progresses in line with the grant process in Paragraph 14.3.	CCS	ATP	CCS redirection	N/A

Use of a Refresh Token

14.9 Where an ATP has been issued with a Refresh Token associated with an active Permission, the ATP may obtain a new Access Token without requiring the Energy Data Subject to re-authenticate, in accordance with the interface table below.

Ref	When	Action	From	To	Interface	Means
14.9.1	As required, where the ATP holds a valid Refresh Token associated with an active Permission.	Submit the Refresh Token to the CCS and request a new Access Token.	ATP	CCS	Refresh Token Request	CCS API
14.9.2	Following 14.9.1.	Validate the Refresh Token and confirm that the associated Permission remains active. Where validation is unsuccessful, proceed to 14.9.3. Where validation is successful, proceed to 14.9.4.	CCS		Internal process	N/A
14.9.3	Following 14.9.2, where the Refresh Token is invalid, expired, revoked or the associated Permission is no longer active.	Reject the request in accordance with the CCS API Technical Specification. The ATP shall initiate a new Permission journey before further Energy Data can be requested.	CCS	ATP	Error codes set out in CCS API Technical Specification	CCS API
14.9.4	Following 14.9.2, where validation is successful.	Issue a new Access Token.	CCS	ATP	Refresh Token Response	CCS API

		Following receipt of replacement Access Token, request Energy Data in accordance with Paragraph 14.3.				

CCS Account Holder Verification

14.10 Where an Energy Supplier is required to carry out Account Holder Verification, it shall do so in accordance with the interface table below

Ref	When	Action	From	To	Interface	Means
14.10.1	As required, where the CCS receives a Pushed Authorization Request requiring Account Holder Verification	Submit request for confirmation that the individual is the relevant Account Holder. The Pushed Authorization Request the CCS issues to the Energy Supplier is constructed by the CCS and requests only the claims necessary to confirm Account Holder status and the associated RMPs.	CCS	Energy Supplier	Pushed Authorization Request (Account Holder Verification Scenario Variant)	CCS API
14.10.2	Following 14.10.1 where the message passes validation.	Return unique reference for the request (request_uri) which the CCS uses to divert the Account Holder to the Energy Supplier.	Energy Supplier	CCS	Pushed Authorization Request Response	CCS API
14.10.3	Following 14.10.2.	Account Holder is redirected to the Energy Supplier portal to authenticate and confirm that Account Holder information and associated RMP details can be shared with the CCS. Where CCS Account Holder Verification is not successful, progress to 14.10.4. Where CCS Account Holder Verification is successful, progress to 14.10.5.	Account Holder	Energy Supplier	Not defined	Energy Supplier Portal

14.10.4	Following 14.10.3, where the Energy Supplier is unable to confirm the individual is the relevant Account Holder.	Provide notification that the CCS Account Holder Verification process has failed.	Energy Supplier	CCS	CCS redirection	N/A
14.10.5	Following 14.10.3. where the Energy Supplier confirms the individual is the relevant Account Holder.	Provide authorization code.	Energy Supplier	CCS	CCS redirection	N/A
14.10.6	Following 14.10.5	Record outcome and use the authorization code via a secure channel to request an Id Token.	CCS	Energy Supplier	Token Request	CCS API
14.10.7	Following 14.10.6 where the message passes validation.	Provide Id Token confirming that the individual is the Account Holder and identifying the RMP(s) against which they are able to provide Permission. The Energy Supplier shall not issue a Refresh Token. The CCS relies on the ID Token only and does not use the Token Response to access any protected resource.	Energy Supplier	CCS	Token Response (Account Holder Verification Scenario Variant)	CCS API
14.10.8	Following 14.10.7.	Record ID Token and progress the Permission journey at the point the Account Holder is requested to confirm whether they wish to provide Permission for the Energy Data to be shared.	CCS		Internal process	N/A

Appendix 1 ATP Energy Data Subject Engagement Requirements

This Appendix includes a checklist of ATP requirements grouped by Permission journey stage, together with generic requirements applicable to all stages. The scope of these requirements is limited to interactions directly related to the process for obtaining Permission to access Energy Data under the CCS Arrangements, and are not intended to apply to any arrangements between the ATP and the Energy Data Subject that extend beyond this scope.

Each ATP requirement is classified as follows:

a. Must – a mandatory requirement that ATPs are required to comply with.

b. Should – a recommendation describing good practice that ATPs are encouraged to adopt where appropriate.

c. May - an optional approach that ATPs may choose to adopt where appropriate.

Stage	ATP Requirement	Obligation level	Checklist
Generic	ATPs must treat Energy Data Subjects fairly, honestly and professionally throughout the CCS journey.	Must	☐
Generic	ATPs must ensure interactions with Energy Data Subjects relating to CCS Permission management are proportionate to the decision being made and support informed Energy Data Subject choice.	Must	☐
Generic	ATPs must not exploit Energy Data Subject inexperience, vulnerability, credulity or loyalty.	Must	☐
Generic	ATPs must provide information that is accurate, complete, clear and not misleading.	Must	☐
Generic	ATPs must provide information that helps Energy Data Subjects understand what data is being shared, why it is being shared, who will receive it and the choices available to them.	Must	☐
Generic	ATPs must enable Energy Data Subjects to verify information relating to their Permission decisions.	Must	☐
Generic	ATPs must support Energy Data Subjects to make Permission decisions freely and with confidence.	Must	☐
Generic	ATPs must not use manipulative, coercive or misleading techniques, including pre-selected options or visual, user interface or user experience design intended to inappropriately influence Energy Data Subject decisions.	Must	☐
Generic	ATPs must explain the consequences of a Permission decision clearly and objectively.	Must	☐
Generic	ATPs must provide Energy Data Subjects with clear and accessible routes to raise questions, concerns, complaints or disputes.	Must	☐
Generic	ATPs must make information about available support easy to find, easy to understand and available at appropriate points throughout the CCS journey.	Must	☐
Generic	ATPs must explain what Energy Data Subjects can expect to happen when a query, concern, complaint or dispute is raised.	Must	☐

Generic	ATPs must ensure that employees and representatives involved in Energy Data Subject-facing interactions understand their responsibilities and are equipped to support Energy Data Subjects appropriately.	Must	☐
Generic	ATPs must ensure that relevant staff understand these ATP requirements, their role in delivering good Energy Data Subject outcomes, and any relevant changes to the CCS arrangements that affect Energy Data Subject-facing interactions.	Must	☐
Generic	ATPs must be able to demonstrate how they meet applicable CCS requirements.	Must	☐
Generic	ATPs must identify, address and escalate risks of Energy Data Subject detriment appropriately to support trust and confidence in the CCS.	Must	☐
Generic	Within the scope of the CCS journey, all Energy Data Subject-facing content must be in plain language that enables Energy Data Subjects to understand the information provided and make informed decisions. ATPs should follow recognised public-sector content design principles, such as the GOV.UK Service Manual guidance on writing for user interfaces.	Must	☐
Generic	Accessibility must be considered at every stage of the CCS journey. Energy Data Subjects may experience different barriers at different moments, depending on the complexity of the task, the channel used, their level of digital confidence, or their personal circumstances at the time. Accessibility requirements apply to all Energy Data Subjects, not just those with identified needs. The Energy Data Subject may face temporary, situational, or permanent barriers. These include reduced cognitive capacity, limited dexterity, low literacy, sensory impairments, and limited English proficiency. ATPs should design Energy Data Subject-facing CCS interactions with this range of barriers in mind.	Must	☐
Generic	All ATP Energy Data Subject-facing screens that form part of the CCS journey should meet WCAG 2.2 AA conformance.	Should	☐
Generic	Where an error prevents completion of a CCS journey, the ATP must provide the Energy Data Subject with a clear explanation of the issue and, where appropriate, the actions available to continue the CCS journey or obtain support.	Must	☐
Generic	The ATP must provide the Energy Data Subject with clear, accessible information explaining how to raise a query, concern or complaint relating to Permission, and expected next steps.	Must	☐

3. Pre-Permission Checklist

Stage	ATP Requirement	Obligation level	Checklist
Pre-Permission	The ATP must explain what the CCS is, and why the Energy Data Subject is being asked to provide Permission.	Must	☐

Pre-Permission	The ATP should surface the tangible personal benefit of data sharing in language relevant to the Energy Data Subject's use case.	Should	☐
Pre-Permission	When identity verification is required by the CCS, the ATP must explain the reason for identity verification, so the Energy Data Subject is prepared.	Must	☐
Pre-Permission	Before initiating the CCS journey, the ATP must inform the Energy Data Subject who is eligible to provide Permission (e.g. Account Holder or Occupier).	Must	☐
Pre-Permission	The ATP must inform the Energy Data Subject that, in the case of a multi-occupancy household, other occupants who are identifiable from the shared data may have the right to request termination of the data sharing, and that it is therefore in the Energy Data Subject's interests to make those occupants aware of the Permission to be provided.	Must	☐
Pre-Permission	The ATP must not provide information that is false or misleading regarding the scope, duration or purpose of the Energy Data sharing before the Energy Data Subject is redirected to the CCS.	Must	☐
Pre-Permission	Before redirecting the Energy Data Subject to the CCS, the ATP must provide a summary of the Permission request, including who is requesting access to the Energy Data, what data will be shared, the purpose(s) and frequency of the data sharing, and the duration of the Permission. The ATP must also explain how the CCS Permission relates to the terms and conditions of the service the ATP is providing.	Must	☐
Pre-Permission	The ATPs may display the CCS Logo in accordance with the terms of the licence set out in the CCS Arrangements Schedule.	May	☐
Pre-Permission	Where an ATP already holds an Energy Data Subject's personal information (for example, name, address, email address or telephone number), the ATP must obtain the Energy Data Subject's agreement before using their information. Where the Energy Data Subject agrees, the ATP should share that information with the CCS to reduce the amount of information the Energy Data Subject needs to enter during the CCS journey.	Must	☐
Pre-Permission	The ATP should signpost its privacy policy and the terms & conditions of the relevant service, before redirecting the Energy Data Subject to CCS.	Should	☐
Pre-Permission	The ATP may provide to the Energy Data Subject a consistent plain-language purpose description aligned to a purpose code included in the Permission request payload.	May	☐
Pre-Permission	The redirect must not disrupt the Energy Data Subject's session context. The Energy Data Subject must be able to return to the ATP after the CCS interaction.	Must	☐

4. Grant Permission Checklist

Stage	ATP Requirement	Obligation level	Checklist

Grant Permission	Where Permission was granted, the ATP may present a clear success outcome screen confirming what happens next.	May	☐
Grant Permission	The ATP must inform the Energy Data Subject which EDH their Energy Data is sourced from, and briefly why that party holds it, as part of the Permission journey.	Must	☐
Grant Permission	Where Permission was not granted, the ATP may present a clear outcome screen reflecting that no Permission was given.	May	☐
Grant Permission	Where the Energy Data Subject does not provide the required Permission through the CCS, and this affects the service that the ATP is able to provide, the ATP should inform the Energy Data Subject of the impact on the service.	Should	☐
Grant Permission	Where withholding/withdrawing Permission affects the ATP's ability to provide a service, the ATP should explain the implications without making Permission a condition for any separate service that does not rely on the relevant Energy Data access.	Should	☐

5. Renew Permission Checklist

Stage	ATP Requirement	Obligation level	Checklist
Renew Permission	The ATP should notify the Energy Data Subject of approaching Permission expiry where the ATP service is enduring beyond the Permission expiry date.	Should	☐
Renew Permission	Where the ATP's service or contract with the Energy Data Subject is ending and renewal is not needed, the ATP may tell the Energy Data Subject that Permission will end along with the contract rather than prompt renewal.	May	☐
Renew Permission	The ATP should explain the consequences of not renewing, which service(s) cease, consistent with revocation-consequence communication.	Should	☐

6. Review Permission Checklist

Stage	ATP Requirement	Obligation level	Checklist
Review Permission	The ATP must enable the Energy Data Subject to easily access and review the status of Permissions relating to that ATP, either through its service or through the CCS Consumer Portal, so that the Energy Data Subject can understand their current Permissions and take action where appropriate, including revoking a Permission.	Must	☐
Review Permission	The ATP must make clear to the Energy Data Subject that it can display only the Permissions granted to that ATP in relation to its own services, and must not imply that it can display Permissions granted to other ATPs. The ATP must provide a link to the CCS Consumer Portal and explain that the Portal enables the Energy Data Subject to view all of their active Permissions across all ATPs.	Must	☐

7. Revoke Permission Checklist

Stage	ATP Requirement	Obligation level	Checklist
Revoke Permission	The ATP must allow revocation of Permission by the Energy Data Subject and may do that within its own service or through the CCS Consumer Portal. Where the revocation is done through the ATP service, the ATP must inform the Energy Data Subject that the CCS Consumer Portal will be updated with this revocation.	Must	☐
Revoke Permission	The ATP should confirm to the Energy Data Subject, through its own service, that access to the Energy Data Subject's Energy Data has stopped following revocation of the Permission.	Should	☐
Revoke Permission	The ATP must ensure Permission is revoked promptly when the basis for accessing the data is no longer applicable.	Must	☐
Revoke Permission	Where Permission is revoked via the ATP's service, the ATP must provide an optional, non-mandatory feedback field for the Energy Data Subject to select a revocation reason from the standardised revocation reasons supported by the CCS. Where the Energy Data Subject does not select a reason, the ATP shall send the applicable default reason.	Must	☐
Revoke Permission	The ATP should explain the consequences of revoking, which service(s) cease, so that the Energy Data Subject can make an informed decision.	Should	☐