Contents

I DATA PRIVACY

I1. DATA PROTECTION AND ACCESS TO DATA

Without Prejudice

I1.1 The obligations of the DCC and each User under this Section I1 are without prejudice to any other obligations they each may have under the Data Protection Legislation and other Relevant Instruments, including any such obligations they each may have concerning Processing of Personal Data.

User Obligations

Consumption Data

I1.2 Each User undertakes that it will not request, in respect of a Smart Metering System, a Communication Service or Local Command Service that will result in it obtaining Consumption Data, unless:

(a) the User has the Appropriate Permission in respect of that Smart Metering System;

(b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System and is relying on paragraph (b) of the definition of Appropriate Permission) the User has, at the point of obtaining Appropriate Permission and at such intervals as are reasonably determined appropriate by the User for the purposes of ensuring that the Energy Consumer is regularly updated of such matters, notified the Energy Consumer in writing of:

(i) the time periods (by reference to length) in respect of which the User obtains or may obtain Consumption Data;

(ii) the purposes for which that Consumption Data is, or may be, used by the User; and

(iii) the Energy Consumer's right to object or withdraw consent (as the case may be) to the User obtaining or using that Consumption Data, and the process by which the Energy Consumer may object or withdraw consent; and

(c) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System and is relying on paragraph (c) of the definition of Appropriate Permission) the User obtains Consumption Data only for (and in accordance with the rights and duties of) the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor and/or Gas Transporter by which the User is contracted (and does not obtain the Consumption Data for any other purpose).

I1.2A If the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor and/or Gas Transporter for a Smart Metering System contracts another User to obtain Consumption Data as envisaged by Section I1.2(c), then both the employing Party and the other User which is providing the service shall be liable for the acts and omissions of such other User in its role as service provider. Without limitation, both the employing Party and such other User shall be in breach of this Code if such other User obtains and/or uses Consumption Data in a manner that breaches the employing Party's Energy Licence or this Code.

I1. Where a User obtains Consumption Data on behalf of an employing Party as envisaged by Section I1.2(c), the User shall only process and use that Consumption Data for the purposes of making it available to the employing Party. The User shall make no other use of the Consumption Data, and shall not process the Consumption Data in any other way (save only that it may retain records of the Consumption Data obtained to the extent it is necessary to do so in order for it to comply with this Code or Laws and Directives).

Service Requests

I1.3 Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless:

(a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or

(b) the Energy Consumer at the premises at which the Smart Meter is located has given the User Unambiguous Consent, which has not been withdrawn, to (as the case may be):

(i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or

(ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible

Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so).

Access to Records

I1.4 Not used.

Reporting Data Breaches

I1.4A This Section I1.4A applies to Consumption Data obtained by a User under Section I1.2(b) or Section I1.2(c). Where the User becomes aware that any such Consumption Data has been disclosed or accessed in breach of this Code, then the User shall:

(a) take all reasonable steps to rectify the cause, and mitigate the impact, of the breach;

(b) unless such breach is unlikely to result in a risk to the rights and freedoms of Energy Consumers, promptly notify the Privacy Sub-Committee of the breach and keep them informed of the steps being taken to rectify the cause, and mitigate the impact, of the breach.

Good Industry Practice

I1.5 Each User shall put in place and maintain arrangements designed in accordance with Good Industry Practice to ensure that each person from whom it has obtained consent pursuant to Section I1.2 to I1.4 is the Energy Consumer.

Processing of Personal Data by the DCC

I1.6 It is acknowledged that, in providing the Services to a User, the DCC may act in the capacity of 'Data Processor' on behalf of that User in respect of the Personal Data for which that User is the 'Data Controller'.

I1.7 The Personal Data which the DCC will Process as a Data Processor on behalf of Users will relate to Energy Consumers, and will include Personal Data which is included within messages sent and received by the DCC via the DCC User Interface or the Self- Service Interface, and/or which is included within messages sent or received by the DCC to or from Communications Hubs. The nature of such Personal Data will be that which is required or permitted to be included in such messages as described in this Code. The full description of the subject matter, the nature and purpose of the processing, and the type of personal data is as described by this Code as a whole.

I1.8 The DCC undertakes for the benefit of each User in respect of the Personal Data for which that User is the 'Data Controller' to:

(a) only Process that Personal Data for the purposes permitted by the DCC Licence and this Code (subject to paragraph (d) below);

(b) only Process that Personal Data for so long as it is required to do so by the DCC Licence and this Code;

(c) undertake the Processing of that Personal Data in accordance with the DCC Licence and this Code, (to the extent consistent with the DCC Licence and this Code) on the documented instructions of the User, and (subject to the foregoing requirements of this Section I1.7(c)) not in a manner that

the DCC knows (or should reasonably know) is likely to cause the User to breach its obligations under the Data Protection Legislation (subject to paragraph (d) below);

(d) if the DCC is aware that, or is of the opinion that, any requirement of paragraph (a) (b) or (c) above infringes the Data Protection Legislation, the DCC shall immediately inform the User of this giving details of the infringement or potential infringement (unless the DCC is prohibited from doing so by any of its other obligations under Laws and Directives);

(e) ensure that the DCC's personnel who are authorised to Process Personal Data are under enforceable obligations of confidentiality and are required only to Process that Personal Data in accordance with the DCC's obligations under the DCC Licence and this Code;

(f) having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement appropriate technical and organisational measures to protect that Personal Data in particular from accidental or unlawful loss, destruction, alteration or unauthorised disclosure of, or access to personal data transmitted, stored or otherwise Processed (such measures to at least be in accordance with Good Industry Practice and the requirements of Section G (Security));

(g) taking into account the nature of the Processing assist the User with its obligations to comply with Data Subjects' requests and Data Subjects' rights under the Data Protection Legislation in respect of that Personal Data through, insofar as is possible, the use of appropriate technical and organisational measures;

(h) taking into account the nature of the Processing and the information available to the DCC, assist the User in ensuring compliance with the User's obligations in Articles 32-36 of the General Data Protection Regulation (or its national equivalent), including:

(i) notifying the User without undue delay if the DCC becomes aware of a breach of the Data Protection Legislation in relation to the Personal Data (including in the event of unauthorised access to such Personal Data); and

(ii) providing full details of the relevant breach where caused by the DCC or any Sub-Processor without undue delay or, where necessary, in phases but always without further undue delay;

(i) provide reasonable assistance to the User in complying with any enquiry made, or investigation or assessment initiated, by the Information Commissioner or any other Competent Authority in respect of the Processing of that Personal Data pursuant to this Code;

(j) promptly notify the User in the event that the DCC Processes any of that Personal Data otherwise than in accordance with this Code (including in the event of unauthorised access to such Personal Data);

(k) notify the User of any complaint relating to the DCC’s obligations under the Data Protection Legislation in respect of the Processing of that Personal Data pursuant to this Code;

(l) after the end of the provision of the Services to which the Processing of that Personal Data relates, at the written election of the User, either securely destroy the Personal Data or return it to the User together with all copies (save to the extent that the DCC is required by Laws and Directives to retain

a copy of the Personal Data) and permit the Independent Privacy Auditor (on the instruction of SECCo on behalf of Users collectively), on giving reasonable prior notice of its intention to audit,

(m) to audit the DCC's compliance with this Section I1.7 during normal business hours, and shall make available to the Independent Privacy Auditor all information, systems and staff reasonably necessary for the Independent Privacy Auditor to conduct such audit. The number of audits shall be limited to no more than once in every twelve (12) calendar month period unless more frequent audits are required under the Data Protection Legislation or the Panel has grounds to suspect there has or is likely to be a breach of the Data Protection Legislation. Where practicable, DCC shall be provided with an opportunity to comment upon the scope of an audit in advance and any audit shall be carried out in such a way that interruption to DCC's operations is minimised as far as is reasonably possible.

DCC's Sub-Processors

I1.9 The DCC shall ensure that its Sub-Processor(s) are subject to written contractual obligations in respect of the Processing of Personal Data which are at least equivalent to the obligations imposed on the DCC under the DCC Licence and this Code, including obligations which provide sufficient guarantees from the Sub-Processor that the Processing meets the requirements stated at any time in the Data Protection Legislation.

I1.10 Each User hereby gives its general authorisation to the DCC to engage Sub-Processor(s) who are appointed in accordance with the DCC Licence and does not object to the engagement by the DCC of any Sub-Processor provided that in engaging the Sub- Processor the DCC complies with the DCC Licence and this Code and publishes on its Website the identity of the Sub-Processor(s) from time to time. Each User hereby consents to Processing by each such Sub-Processor who is appointed in accordance with the DCC Licence and this Code.

Records

I1.11 The DCC and each User will each maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the DCC and each such User to demonstrate that it is complying with its respective obligations under Sections I1.2 to I1.9.

I1.12 The DCC shall make available to each User all information reasonably necessary to demonstrate compliance by the DCC with Sections I1.6 to I1.9, but only insofar as such information relates to the Personal Data for which that User is the Data Controller.

General Compliance with Data Protection Legislation

I1.13 Each of the DCC, SECCo, and each User undertakes to comply with its obligations under the Data Protection Legislation in respect of Personal Data they Process as a Data Controller or Data Processor pursuant to this Code.

Permission for Gas Supplier to Store Data on Shared SMETS1 Installation

I1.14 In the case of a SMETS1 GSME which forms part of the same SMETS1 Installation as a SMETS1 ESME, and where the Gas Supplier for the SMETS1 GSME is a different person to the Import Supplier for the SMETS1 ESME, the Import Supplier hereby agrees to permit the Gas Supplier to store Data on the SMETS1 GPF which forms part of that SMETS1 Installation in the manner envisioned by SMETS1.

I2. OTHER USER PRIVACY AUDITS

Procurement of the Independent Privacy Auditor

I2.1 The Panel shall procure the provision of privacy audit services:

(a) of the scope specified in Section I2.3;

(b) from a person who:

(i) is suitably qualified, and has the necessary experience and expertise, to provide those services; and

(ii) is suitably independent in accordance with Section I2.4,

and that person is referred to in this Section I2 as the "**Independent Privacy Auditor**".

I2.2 The Panel may appoint more than one person to carry out the functions of the Independent Privacy Auditor.

Scope of Privacy Audit Services

I2.3 The privacy audit services specified in this Section I2.3 are services in accordance with which, for the purpose of providing reasonable assurance that Other Users are complying with their obligations under Sections I1.2 to I1.5 (User Obligations), the Independent Privacy Auditor shall:

(a) carry out Privacy Assessments at such times and in such manner as is provided for in this Section I2;

(b) produce Privacy Assessment Reports in relation to Other Users that have been the subject of a Privacy Assessment;

(c) receive and consider Privacy Assessment Responses;

(d) otherwise, at the request of, and to an extent determined by, the Panel carry out an assessment of the compliance of any Other User with its obligations under Sections I1.2 to I1.5;

(e) provide to the Panel such advice and support as may be requested by it from time to time, including in particular advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(f) provide to the Authority such advice and support as it may request in relation to any disagreements with a decision of the Panel in respect of which the Authority is required to make a determination in accordance with this Section I2; and

(g) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section I2.

Independence Requirement

I2.4 The Independent Privacy Auditor shall be treated as suitably independent in accordance with this Section I2.4 only if it satisfies:

(a) the requirements specified in Section I2.6; and

(b) the requirement specified in Section I2.7.

I2.5 For the purposes of Sections I2.6 and I2.7:

(a) a "**Relevant Party**" means any Party in respect of which the Independent Privacy Auditor carries out functions under this Section I2; and

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as an Other User under Section I1.2 to I1.5.

I2.6 The requirements specified in this Section I2.6 are that:

(a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent Privacy Auditor;

(b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent Privacy Auditor; and

(c) the Independent Privacy Auditor does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the Independent Privacy Auditor where it acts in that capacity).

I2.7 The requirement specified in this Section I2.7 is that the Independent Privacy Auditor is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the Independent Privacy Auditor itself being a Relevant Service Provider to any Relevant Party).

Compliance of the Independent Privacy Auditor

I2.8 The Panel shall be responsible for ensuring that the Independent Privacy Auditor carries out its functions in accordance with the provisions of this Section I2.

Other Users: Duty to Cooperate in Assessment

I2.9 Each Other User shall do all such things as may be reasonably requested by the Panel, or by any person acting on behalf of or at the request of the Panel (including in particular the Independent Privacy Auditor), for the purposes of facilitating an assessment of that Other User's compliance with its obligations under Sections I1.2 to I1.5.

I2.10 For the purposes of Section I2.9, an Other User shall provide the Panel (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that Other User as are used for, and such persons engaged by that Other User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections I1.2 to I1.5; and

(ii) such cooperation as may reasonably by requested by the Independent Privacy Auditor for the purposes of carrying out any Privacy Assessment in accordance with this Section I2.

Categories of Assessment

I2.11 I2.11 For the purposes of this Section I2, there shall be the following three categories of privacy assessment:

(a) a Full Privacy Assessment (as further described in Section I2.12);

(b) a Random Sample Privacy Assessment (as further described in Section I2.13); and

(c) a Privacy Self-Assessment (as further described in Section I2.14).

I2.12 A "**Full Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to which that Other User:

(a) is compliant with each of its obligations under Sections I1.2 to I1.5; and

(b) has in place the systems and processes necessary for ensuring that it complies with each such obligation.

I2.13 A "**Random Sample Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to which the Other User is compliant with each of its obligations under Sections I1.2 to I1.5 in relation to a limited (sample) number of Energy Consumers.

I2.14 A " **Privacy Self-Assessment**" shall be an assessment carried out by an Other User to identify the extent to which, since the last occasion on which a Privacy Assessment was carried out in respect of that Other User by the Independent Privacy Auditor, there has been any material change:

(a) in the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) in the quantity of Consumption Data being obtained by the Other User.

The Privacy Controls Framework

I2.15 The Privacy Sub-Committee shall develop and maintain a document to be known as the "**Privacy Controls Framework**" which shall:

(a) set out arrangements designed to ensure that Privacy Assessments are carried out appropriately for the purpose of providing reasonable assurance that Other Users are complying with (or, for the

purposes of Section H1.10(d) (User Entry Process Requirements), are capable of complying with) their obligations under Sections I1.2 to I1.5;

(b) for that purpose, in particular, specify the principles and criteria to be applied in the carrying out of any Privacy Assessment, including principles designed to ensure that Privacy Assessments take place on a consistent basis across all Other Users; and

(c) make provision for determining the timing, frequency and selection of Other Users for the purposes of Random Sample Privacy Assessments.

I2.16 In developing the Privacy Controls Framework, and prior to making any subsequent change to it, the Privacy Sub-Committee shall consult with and have regard to the views of all Parties, Citizens Advice and Consumer Scotland, and the Authority.

I2.17 The Privacy Sub-Committee shall ensure that an up to date copy of the Privacy Controls Framework is made available to all Parties and is published on the Website.

Privacy Assessments: General Procedure

Privacy Controls Framework

I2.18 Each Privacy Assessment carried out by the Independent Privacy Auditor or an Other User shall be carried out in accordance with the Privacy Controls Framework.

The Privacy Assessment Report

I2.19 Following the completion of a Full Privacy Assessment or Random Sample Privacy Assessment, the Independent Privacy Auditor shall, in discussion with the Other User to which the assessment relates, produce a written report (a "**Privacy Assessment Report**") which shall:

(a) set out the findings of the Independent Privacy Auditor on all the matters within the scope of the Privacy Assessment;

(b) specify any instances of actual or potential non-compliance of the Other User with its obligations under Sections I1.2 to I1.5 which have been identified by the Independent Privacy Auditor;

(c) set out the evidence which, in the opinion of the Independent Privacy Auditor, establishes each of the instances of actual or potential non-compliance which it has identified.

I2.20 The Independent Privacy Auditor shall submit a copy of each Privacy Assessment Report to the Privacy Sub-Committee and to the Other User to which that report relates.

The Privacy Assessment Response

I2.21 Following the receipt by any Other User of a Privacy Assessment Report which relates to it, the Other User shall as soon as reasonably practicable, and in any event by no later than such date as the Privacy Sub-Committee may specify:

(a) produce a written response to that report (a "**Privacy Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Privacy Sub-Committee and the Independent Privacy Auditor.

I2.22 Where a Privacy Assessment Report specifies any instance of actual or potential non- compliance of an Other User with its obligations under Sections I1.2 to I1.5, the Other User shall ensure that its Privacy Assessment Response includes the matters referred to in Section I2.23.

I2.23 The matters referred to in this Section are that the Privacy Assessment Response:

(a) indicates whether the Other User accepts the relevant findings of the Independent Privacy Auditor and provides an explanation of the actual or potential non-compliance that has been identified; and

(b) sets out any steps that the Other User proposes to take in order to remedy and/or mitigate the actual or potential non-compliance, and identifies a timetable within which the Other User proposes to take those steps.

I2.24 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), the Privacy Sub-Committee (having considered the advice of the Independent Privacy Auditor) shall review that response and either:

(a) notify the Other User that it accepts that the steps that the Other User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance specified in the Privacy Assessment Report; or

(b) seek to agree with the Other User such alternative steps and/or timetable as would, in the opinion of the Privacy Sub-Committee, be more appropriate for that purpose.

I2.25 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Privacy Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the Other User in accordance with Section I2.24, the Other User shall:

(a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Privacy Sub-Committee:

(i) on its progress in taking those steps, at any such intervals or by any such dates as the Privacy Sub-Committee may specify;

(ii) on the completion of those steps in accordance with the timetable; and

(iii) on any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

The Privacy Self-Assessment Report

I2.26 Following the completion of a Privacy Self-Assessment, the Other User which carried out that self-assessment shall as soon as reasonably practicable produce a written report (a "**Privacy Self-Assessment Report**") which shall set out the findings of the Other User, and describe the nature of any material change, since the last occasion on which a Privacy Assessment was carried out in respect of the Other User by the Independent Privacy Auditor, in respect of:

(a) the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) the quantity of Consumption Data being obtained by the Other User.

I2.27 A Other User which produced a Privacy Self-Assessment Report shall:

(a) ensure that the report is accurate, complete and not misleading; and

(b) submit a copy of the report to the Privacy Sub-Committee and the Independent Privacy Auditor.

I2.28 Within the period of time specified in the Privacy Controls Framework following the receipt by it of a Privacy Self-Assessment Report, the Independent Privacy Auditor shall either:

(a) notify the Other User that it accepts that report; or

(b) inform the Other User that it will be subject to an additional Privacy Assessment of such nature by such date as the Privacy Sub-Committee may specify.

Initial Full Privacy Assessment: User Entry Process

I2.29 Sections I2.31 to I2.36 set out the applicable privacy requirements referred to in Section H1.10(d) (User Entry Process Requirements).

I2.30 For the purposes of Sections I2.31 to I2.36, any reference in Sections I1.2 to I1.5 or the preceding provisions of this Section I2 to a 'User' or 'Other User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for the User Role of Other User.

Initial Full Privacy Assessment

I2.31 For the purpose of completing the User Entry Process for the User Role of Other User, a Party wishing to act in that User Role shall be subject to a Full Privacy Assessment.

Privacy Sub-Committee: Setting the Assurance Status

I2.32 Following the receipt by it of the Privacy Assessment Report and Privacy Assessment Response produced after the initial Full Privacy Assessment, the Privacy Sub-Committee shall promptly consider both documents and set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections I1.2 to I1.5, in accordance with Section I2.33.

I2.33 The Privacy Sub-Committee shall set the assurance status of the Party as one of the following:

(a) approved;

(b) approved, subject to the Party:

(i) taking such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b); or

(ii) both taking such steps and being subject to a further Privacy Assessment of such nature and by such date as the Privacy Sub-Committee may specify;

(c) deferred and:

(i) the Party having first taken such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b) and been subject to a further Privacy Assessment; and

(ii) the Privacy Sub-Committee having determined that it is satisfied, on the evidence of the further Privacy Assessment, that such steps have been taken; or

(d) rejected and:

(i) the Party shall have a second Full Privacy Assessment to address any issues identified by the Privacy Sub-Committee as being, in the opinion of the Panel, not adequately addressed in that response as submitted to Panel; and

(ii) upon completion of the second Full Privacy Assessment the Privacy Sub-Committee will reconsider the assurance status in accordance with Section I2.32.

Approval

I2.34 For the purposes of Sections H1.10(d) and H1.11 (User Entry Process Requirements):

(a) a Party shall be considered to have successfully demonstrated that it meets the applicable privacy requirements of this Section I2 when:

(i) the Privacy Sub-Committee has set its assurance status to 'approved' in accordance with either Section I2.33(a) or (b); or

(ii) the Privacy Sub-Committee has set its assurance status to 'deferred' in accordance with Section I2.33(c) and the requirements specified in that Section have been met; and

(b) the Privacy Sub-Committee shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

I2.35 Where the Privacy Sub-Committee has set the assurance status of a Party to 'approved subject to' specified in Section I2.33(b), the Party shall take the steps to which that approval is subject in accordance with that section.

Disagreement with Privacy Sub-Committee Decisions

I2.36 Where a Party disagrees with any decision made by the Privacy Sub-Committee in relation to it under Section I2.33, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Privacy Assessments: Post-User Entry Process

I2.37 Following its initial Full Privacy Assessment for the purposes of the User Entry Process, an Other User shall be subject to annual Privacy Assessments as follows:

(a) in the first year after the year of its initial Full Privacy Assessment, to a Privacy Self-Assessment;

(b) in the immediately following year, to a Privacy Self-Assessment;

(c) in the next following year, to a Full Privacy Assessment; and

(d) in each year thereafter, to a category of Privacy Assessment which repeats the same annual sequence as that of paragraphs (a) to (c),

but these requirements shall be subject to the provisions of Section I2.38.

I2.38 An Other User:

(a) may, on the instruction of the Privacy Sub-Committee, or otherwise in accordance with the provisions of the Privacy Controls Framework, be subject to a Full Privacy Assessment or Random Sample Privacy Assessment at any time; and

(b) where it is subject to such a Privacy Assessment in a year in which it would otherwise have been required to carry out a Privacy Self-Assessment in accordance with Section I2.37, shall not be required to carry out that self-assessment in that year.

Privacy Self-Assessment

I2.39 Where, in accordance with the requirements of this Section I2, an Other User is subject to a Privacy Self-Assessment in any year, that Other User shall:

(a) carry out the Privacy Self-Assessment during that year;

(b) do so in accordance with the Privacy Controls Framework; and

(c) ensure that the outcome of the Privacy Self-Assessment is documented and is submitted to the Independent Privacy Auditor for review by no later than the date which is 13 months after the date of the commencement of the previous Full Privacy Assessment or (if more recent) Privacy Self-Assessment.

Other Users: Obligation to Pay Explicit Charges

I2.40 Each Other User shall pay to the DCC all applicable Charges in respect of:

(a) all Privacy Assessments carried out in relation to it by the Independent Privacy Auditor;

(b) the production by the Independent Privacy Auditor of any Privacy Assessment Reports following such assessments; and

(c) all related activities of the Independent Privacy Auditor in respect of that Other User in accordance with this Section I2.

I2.41 Expenditure incurred in relation to Other Users in respect of the matters described in Section I2.40 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

I2.42 For the purposes of Section I2.40 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

(a) the expenditure incurred in respect of the matters described in Section I2.40 that is attributable to individual Other Users, in order to facilitate Explicit Charges designed to pass-through the expenditure to such Other Users pursuant to Section K7 (Determining Explicit Charges); and

(b) any expenditure incurred in respect of the matters described in Section I2.40 which cannot reasonably be attributed to an individual Other User.

I3. Establishment of the Privacy Sub-Committee

Establishment of the Privacy Sub-Committee

I3.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section I3, to be known as the **"Privacy Sub-Committee"**.

I3.2 Save as expressly set out in this Section I3, the Privacy Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the Privacy Sub-Committee

I3.3 The Privacy Sub-Committee shall be composed of the following persons (each a **"Privacy Sub-Committee Member"**):

(a) the Privacy Sub-Committee Chair (as further described in Section I3.5);

(b) eight Privacy Sub-Committee (Supplier) Members (as further described in Section I3.6);

(c) two Privacy Sub-Committee (Network) Members (as further described in Section I3.8);

(d) three Privacy Sub-Committee (Other User) Members (as further described in Section I3.10);

(e) one person acting as Consumer Representative (nominated jointly by Citizens Advice and Consumer Scotland;) (as further described in Section I3.13); and

(f) one representative of the DCC (as further described in Section I3.14).

I3.4 Each Privacy Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Privacy Sub-Committee Member at the same time.

I3.5 The **"Privacy Sub-Committee Chair"** shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Privacy Sub-Committee Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the Privacy Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Privacy Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members); and

(e) provision is made for the Privacy Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

I3.6 Each of the eight **"Privacy Sub-Committee (Supplier) Members"** shall;

(a) be appointed in accordance with Section I3.7 subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Privacy Sub-Committee (Supplier) Member", references to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", and references to "Panel Members" were to "Panel Sub-Committee Members".

I3.7 Each of the eight Privacy Sub-Committee (Supplier) Members shall (subject to Section I3.12) be appointed in accordance with a process:

(a) by which six Privacy Sub-Committee (Supplier) Members will be elected by Large Supplier Parties, and two Privacy Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", references to "Panel Members" were to "Privacy Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section I3).

I3.8 Each of the two **"Privacy Sub-Committee (Network) Members"** shall:

(a) be appointed in accordance with Section I3.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Privacy Sub-Committee (Network) Member", references to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", and references to "Panel Members" were to "Privacy Sub-Committee Members".

I3.9 Each of the two Privacy Sub-Committee (Network) Members shall (subject to Section I3.12) be appointed in accordance with a process:

(a) by which one Privacy Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Privacy Sub-Committee (Network) Member will be elected by the Gas Network Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", references to "Panel Members" were to "Privacy Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section I3).

I3.10 Each of the three **"Privacy Sub-Committee (Other User) Members"** shall:

(a) be appointed in accordance with Section I3.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Privacy Sub-Committee (Other User) Member", references to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", and references to "Panel Members" were to "Privacy Sub-Committee Members".

I3.11 Each of the three Privacy Sub-Committee (Other User) Members shall (subject to Section I3.12) be appointed in accordance with a process:

(a) by which three Privacy Sub-Committee (Other User) Members will be elected by the Other SEC Parties which are eligible to act in the role of Other User; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", references to "Panel Members" were to "Privacy Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section I3).

I3.12 The following shall apply in respect of all candidates nominated or re-nominated for election as a Privacy Sub-Committee (Supplier) Member, Privacy Sub-Committee (Network) Member or Privacy Sub-Committee (Other User) Member.

(a) the Privacy Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Privacy Sub-Committee determines that the candidate does not satisfy one or more of the following requirements:

(i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;

(ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant privacy expertise in relation to the category of membership of the Privacy Sub-Committee for which the candidate has been nominated; and

(iii) the candidate must have sufficient privacy expertise in relation to the category of membership of the Privacy Sub-Committee for which the candidate has been nominated;

(b) a candidate who is rejected under paragraph (a) above shall not (subject to paragraph (c) below) be an eligible candidate for the relevant election;

(c) where a candidate disputes a rejection notification under paragraph (a) above, the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in paragraph (a) above; and

(d) where necessary, the Secretariat shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in paragraph (a) and/or (c) or determination by the Panel under paragraph (c) (as applicable).

I3.13 The Consumer Representative (nominated jointly by Citizens Advice and Consumer Scotland) may nominate one person to be a Privacy Sub-Committee Member by notice to the Secretariat from time to time. The Consumer Representative may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

I3.14 The DCC may nominate one person to be a Privacy Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Privacy-Sub Committee

I3.15 Subject to Sections I3.16, I3.17, I3.18 and I3.19, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Privacy Sub-Committee, for which purpose that Section shall be read as if references to "Panel" were to "Privacy Sub-Committee", references to "Panel Chair" were to "Privacy Sub-Committee Chair", and references to "Panel Members" were to "Privacy Sub-Committee Members".

I3.16 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section I3.15:

(a) a representative of the Secretary of State and a representative of the Authority shall be:

(i) invited to attend each and every Privacy Sub-Committee meeting;

(ii) entitled to speak at such Privacy Sub-Committee meetings without the permission of the Privacy Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Privacy Sub-Committee Members in respect of such meetings; an

(b) the Privacy Sub-Committee Chair shall invite to attend Privacy Sub-Committee meetings any persons that the Privacy Sub-Committee determines it appropriate to invite in order to be provided with expert advice on privacy matters.

Duties and Powers of the Privacy Sub-Committee

I3.17 The Privacy Sub-Committee:

(a) shall perform the duties and may exercise the powers set out in Sections I3.21 to I3.28 (inclusive); and

(b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Privacy Sub-Committee elsewhere in this Code.

Document Development and Maintenance

I3.18 The Privacy Sub-Committee shall:

(a) maintain the Privacy Controls Framework;

(b) carry out a review of the Privacy Assessment process at least once each year in order to ensure it continues to provide an appropriate level of assurance that privacy and data protection risks are appropriately mitigated and reflecting any improvements or amendments to this Code and/or the Privacy Controls Framework;

(c) develop and maintain an Unambiguous Consent strategy setting out requirements for collecting, maintaining and processing consent and withdrawal of consent, in support of Section I1.4 (Access to Records);

(d) maintain the definition of Good Industry Practice, in support of Section I1.5 (Good Industry Practice);

(e) maintain the definition of materiality in respect of Users' processes in support of Section I2.26 (Privacy Self-Assessment Report);

(f) provide such guidance on Data Protection Legislation as it determines may be necessary from time to time, in support of Section I1.12 (General Compliance with Data Protection Legislation);

(g) maintain a statement of privacy objectives aligned to the SEC Objectives for use when assessing the continued effectiveness of the Privacy Controls Framework and Privacy Assessment process; and

(h) maintain and implement a memorandum of understanding with the Information Commissioner in relation to privacy and this Code.

Privacy Assurance

I3.19 The Privacy Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the privacy-related obligations and assurance arrangements under this Code in order to identify whether in the opinion of the Privacy Sub-Committee they continue to be fit for purpose;

(b) periodically, and in any event at least once each year, carry out reviews of the Privacy Assessment scope, as follows:

(i) Full Privacy Assessments, to ensure they continue to meet the objectives set out in Section I2.12;

(ii) Privacy Self-Assessments, to ensure they continue to meet the objectives set out in Section I2.14; and

(iii) Random Sample Privacy Assessments, to ensure they continue to meet the objectives set out in Section I2.13.

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of this Code concerning privacy;

(d) shall to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a Privacy Assessment Response that sets out any steps that the User proposes to take in accordance with Section I2.33(b); liaise with that User (or Party) as to the nature and timetable of such steps;

(e) provide advice to the Panel on the scope and output of the independent privacy assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;

(f) provide advice to the Panel in relation to the appointment of the Independent Privacy Auditor, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance;

(g) provide advice and information to the Information Commissioner and the Authority via the Panel in relation to any actual or potential non-compliance with Data Protection Legislation in the event of a material concern arising from a privacy assessment; and

(h) liaise with the Information Commissioner at such meetings and in such manners as may be scheduled under the terms of the memorandum of understanding with the Information Commissioner.

Monitoring and Advice

I3.20 The Privacy Sub-Committee shall:

(a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of data privacy incidents and the management of notifications and regulator liaison;

(b) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to Section I (Data Privacy);

(c) provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect data privacy;

(d) respond to any consultations on matters which may affect the data privacy or the effective implementation of the privacy controls under this Code;

(e) act in cooperation with, and send a representative to any Sub-Committee or Working Group which requests the support or attendance of the Privacy Sub-Committee;

(f) provide guidance to the Panel on data ethics and publish such guidance on data ethics as it may determine appropriate from time to time;

(g) considering and responding to privacy implications of emerging and novel technologies such as artificial intelligence; and

(h) provide such further support and advice to the Panel, the Authority and other Parties as may be requested.

Modifications

I3.21 The Privacy Sub-Committee shall establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Privacy Sub-Committee) those proposals that:

(a) are likely to affect the privacy assurance arrangements under Section I2 (Other User Privacy Audits); or

(b) are likely to relate to other parts of the Code but may have a material effect on Data privacy.

I3.22 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals), the Privacy Sub-Committee shall be entitled to submit Draft Proposals in respect of Section I (Data Privacy) where the Privacy Sub-Committee considers it appropriate to do so.

I3.23 Notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Privacy Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

I3.24 For the purposes of Section D7.1 (Modification Report):

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by

(i) the Privacy Sub-Committee; and/or

(ii) any Privacy Sub-Committee member.

(b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.