North Somerset Council Energy Management Contract Z Clauses

ZM1: Compliance with the Public Contracts Regulations 2015

ZM1.1 (1)The *Client* may terminate the *Consultant*'s obligation to Provide the Service if any of the provisions of paragraph 73(1) of The Public Contracts Regulations 2015 apply.

If the *Client* terminates under the provisions of paragraph 73(1)(b) of the Public Contracts Regulations 2015 as a result of information not disclosed by the *Consultant* at the Contract Date, the procedures and amounts due on termination are the same as if the *Consultant* has substantially failed to Provide the Service.

If the *Client* otherwise terminates under the provisions of paragraph 73(1) of the Public Contracts Regulations 2015, the procedures and amounts due on termination are the same as if the Parties had been released under the law from further performance of the whole of this contract.

(2) The *Consultant* does not appoint a Subcontractor or supplier if there are compulsory grounds for excluding the Subcontractor or supplier under regulation 57 of the Public Contracts Regulations 2015.

(3) The *Consultant* includes in any subcontract awarded by him provisions requiring that:

• payment due to the Subcontractor or supplier under the subcontract is made no later than 30 days after receipt of a valid and undisputed invoice, unless this contract requires the *Consultant* to make earlier payment to the Subcontractor,
• invoices for payment submitted by the Subcontractor are considered and verified by the *Consultant* in a timely fashion,
• undue delay in considering and verifying invoices is not sufficient justification for failing to regard an invoice as valid and undisputed and
• any contract awarded by the Subcontractor for work included in this contract includes provisions to the same effect as these provisions.

ZM2: Fair payment

ZM2.1 "Fair Payment Charter" is the model form of fair payment charter originally published by the Office of Government Commerce (now adopted by the Cabinet Office) and based upon the "Guide to Best Fair Payment Practices."

ZM2.2 The *Consultant* applies the Fair Payment Charter to his Subcontractors and suppliers (of all tiers) involved in Providing the Service.

ZM3: Conflict of interest

ZM3.1 The *Consultant* notifies the *Service Manager* as soon as he becomes aware of any circumstances giving rise to, or potentially giving rise to, conflicts of interest relating to the *Consultant* or the *Client* (including, without limitation, conflicts affecting the *Client's* reputation and standing) which the *Consultant* anticipates may justify the *Client* taking action to protect his interests.

ZM8: Reasons for termination

ZM8.1 Delete clause 91.5 and add the following.

91.5 Either Party may terminate if the Parties (R17)

- have been released under the law from further performance of the whole of this contract or
- are unable either to remove a conflict of interest or to reduce its damaging effect to a mutually acceptable level.

ZM9: Intellectual Property Rights

ZM9.1 Intellectual Property Rights are all patents, trademarks, service marks, copyright, moral rights, rights in design, rights in databases, know-how and all or any other intellectual or industrial property rights whether or not registered or capable of registration in the United Kingdom or any other part of the world, together with all or any related good will.

ZM9.2 All Intellectual Property Rights in any existing Information and Communication Technology (ICT) or other systems operated by the *Client* and documents prepared by the *Client* remain vested in the *Client* and the *Consultant* provides all reasonable assistance to the *Client* in the protection of the vesting of such Intellectual Property Rights in the *Client*.

ZM9.3 In relation to any ICT or other systems used and/or developed by the *Consultant* for the purposes of this contract, all Intellectual Property Rights in such systems that are developed during the contract for the

benefit of the *Client* vest in the *Client* save to the extent referred to in clauses ZM9.5 and ZM9.6.

ZM9.4 In relation to any documents prepared by or on behalf of the *Consultant* for the purposes of Providing the Service or in connection with this contract, the *Consultant* grants or procures for the benefit of the *Client* an irrevocable royalty free licence to use and reproduce the documents for the same or similar purposes to those originally intended, whether before or after the Completion. The licence includes the right, at no charge to the *Client,* to grant sub-licences and is transferable to third parties.

ZM9.5 To the extent that any of the documents referred to in clause ZM9.4 is generated by, or maintained on, a computer or other equipment or otherwise in any machine readable format, the *Consultant* procures for the benefit of the *Client*, the grant of a licence or sub-licence for, and supply of, any relevant software or database to enable the *Client* or any person authorised by it to access and otherwise use such data for the same or similar purposes to those originally intended.

ZM9.6 To the extent that any ICT or other systems used by the *Consultant* for the purposes of this contract were developed by the *Consultant* before entering into this contract, the Intellectual Property Rights in such ICT or other systems remain vested in the *Consultant* provided that the *Consultant* procures for the *Client* the grant of the rights referred to in clause ZM9.5 if and to the extent that the relevant ICT or other systems are necessary to the successful continued operation of the *service* provided, or previously provided, under this contract.

ZM10: Confidentiality

ZM10.1 **Keep Confidential**
Confidential Information is information, the disclosure or use of which would constitute an actionable breach of confidence, which has either been notified as confidential by either Party in writing or that ought reasonably to be considered as confidential, which relates to the business affairs, trade secrets, intellectual property rights or know-how of either Party and/or personal data and sensitive personal data within the meaning of the General Data Protection Regulation.

ZM10.2 The Parties do not disclose or use Confidential Information except;

- as required and necessary in connection with the *service*,

- where already in the public domain or in the possession of the other Party, other than as a result of a Party breaching this contract,

- for the purpose of dispute resolution in connection with this contract,

- in accordance with the *law of the contract* or

- as necessary for the *Service Manager* to validate the *Consultant's* accounts and records of Defined Cost.

ZM10.3 **Obligation preserved**
If disclosure or use of Confidential Information is permitted, the disclosing Party places the receiver under the same obligation of confidentiality required by this contract.

ZM12: Freedom of Information

ZM12.1 The Parties acknowledge that the FOI and EIR may apply to this contract. The Parties undertake to facilitate compliance with the information disclosure requirements pursuant to the FOI and EIR in the manner provided for in clauses ZM12.2 and ZM12.3 to the extent that such requirements relate to information held by a Party on behalf of the other Party in connection with this contract.

ZM12.2 Request for Information has the meaning set out in section 8 of the FOI.

ZM12.3 Before responding to a Request for Information, the *Client* will consider in its absolute discretion

- the availability of exemptions under the FOI, the EIR or any other applicable legislation and

- where an exemption being considered requires it, whether or not the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing information relating to this contract.

ZM12.4 Before

- responding to a Request for Information (which, where the FOI or EIR provides, includes confirming or denying that the information is held by the *Client* or on the *Client's* behalf) or

- disclosing information about, or relating to, this contract

the *Client* notifies the *Consultant* of the Request for Information and stipulates the time period (not exceeding one week from the date of the Request for Information) within which the *Consultant* must make representations to the *Client* concerning whether an exemption applies (including, where necessary, why the public interest in maintaining the exemption is not outweighed by the public interest in disclosure).

ZM12.5 In determining whether an exemption applies or whether to confirm or deny or to disclose any information, the *Client* takes into account any reasonable representations made by the *Consultant*.

ZM12.6 The *Consultant* acknowledges that, acting in accordance with the Secretary of State for Constitutional Affairs' Code of Practice on the Discharge of Public Authorities' Functions under Part 1 of the FOI, the *Client* may be obliged, or in its discretion decide, under the FOI or EIR to disclose information concerning this contract

- without consulting with the *Consultant* or
- following consultation with the *Consultant* and having taken its views into account.

A disclosure made in accordance with the FOI or EIR is not in breach of any confidentiality agreements between the Parties.

ZM13: Data Protection

ZM13.1 The Parties comply with the provisions of Schedule 2 – Data Protection Schedule

ZM15: Equality Act

ZM15.1 The *Consultant* does not discriminate directly or indirectly or by way of victimisation or harassment against any person contrary to the Equality Act 2010.

ZM15.2 Where possible in Providing the Service, the *Consultant* co-operates with and assists the *Client* to satisfy his duty under the Equality Act 2010 to eliminate unlawful discrimination and to promote equality of opportunity between persons of different racial groups and between disabled people and other people.

ZM15.3 Where any employee or Subcontractor employed by the *Consultant* is required to carry out any Services in any Client's premises, the

Consultant ensures that each such employee or Subcontractor complies with the *Client's* employment policies and codes of practice relating to discrimination and equal opportunities.

M15.4 The *Consultant* notifies the *Service Manager* in writing as soon as he becomes aware of any investigation or proceedings brought against the *Consultant* under the Equality Act 2010 in connection with this contract and

- provides any information requested by the investigating body, court or tribunal in the timescale allotted,
- attends (and permits a representative from the *Client* to attend) any associated meetings,
- promptly allows access to any relevant documents and information and
- cooperates fully and promptly with the investigatory body, court or tribunal.

ZM15.5 The *Consultant* indemnifies the *Client* against all costs, charges, expenses (including legal and administrative expenses) and payments made by the *Client* arising out of or in connection with any investigation or proceedings under the Equality Act 2010 resulting from any act or omission of the *Consultant*.

ZM16: Human Rights

ZM16.1 The *Consultant* shall comply in all respects with the provision of the Human Rights Act 1998 and will indemnify the *Client* against all actions, costs, expenses, claims, proceedings and demands which may be brought against the *Client* for a breach of statutory duty under the Act attributable to the *Consultant*.

ZM16.2 The *Consultant* shall comply with the Modern Slavery Act 2015 and where applicable implement a due diligence procedure for its own suppliers, Subcontractors and other participants in its supply chain to ensure that there is no slavery or human trafficking in its supply chain.

ZM17: Complaints and Regulatory Actions

ZM17.1 Where any investigation by a Local Government Ombudsman or any other regulator or investigatory authority of competent jurisdiction takes place, the *Consultant*

- attends meetings as required by the Ombudsman, regulator or investigatory authority and requires its personnel and

Subcontractors to attend meetings or interviews if reasonably necessary,

- promptly allows access to and investigation of any documents deemed by the Ombudsman, regulator or investigatory authority to be relevant,
- allows any of its personnel or Subcontractors to appear as a witness in any proceedings and
- co-operates as required by the Ombudsman, regulator or investigatory authority during the course of any investigation.

ZM17.2 The *Consultant* keeps a record of any complaints received (whether received orally or in writing, and whether from members of the *Client*, members of the public or otherwise) and of the action taken by the *Consultant* to remedy or fully investigate each such complaint. Such records shall be kept available for inspection by the *Client* at all reasonable times during normal working hours.

ZM18: Assignment

ZM18.1 The *Consultant* does not assign, novate or otherwise dispose of this contract or any part thereof without the prior consent in writing of the *Client*.

ZM21: Poaching of Employees

ZM21.1 For a period of 12 months after Completion neither the *Client* nor the Consultant seeks to poach the other Party's staff (either directly employed or subcontracted) who are or have been associated with the procurement and/or operation of the contract provided that neither of the Parties is prevented from employing a former employee of the other who responds to a bona fide advertisement.

ZM22: Whistleblowing

ZM22.1 The *Consultant* confirms that the *Client* is authorised as a person to whom the *Consultant's* staff may make a qualifying disclosure under the Public Interest Disclosure Act 1998 and declares that any of its staff making a protected disclosure (as defined by the said Act) is not subjected to any detriment and its staff are made aware of this provision.

ZM22.2 The *Consultant* maintains and reviews its whistleblowing policy and procedure on a periodic basis in accordance with good industry practice.

ZM23: Tax Compliance

ZM23.1 Where VAT is chargeable in respect of the service, the *Consultant* shall calculate the amount of VAT to be paid by the Client at the applicable prevailing rate, which shall be added to the Charges and paid by the Client following the submission of a VAT invoice by the *Consultant* in respect of the same.

ZM23.2 The *Consultant* shall indemnify the *Client* against any liability (including any interest, penalties or costs incurred) which is levied, demanded or assessed on the *Client* at any time in respect of the *Consultant's* failure to account for, or to pay, any VAT relating to payments made to the *Consultant* under this Agreement.

ZM23.3 The *Consultant* acknowledges the *Client* is a public authority and has a duty to promote compliance with all relevant tax laws through its supply chain. The *Consultant* promptly notifies the *Client* if it has grounds to consider that a potential non-compliance with a relevant tax law may have occurred in respect of the service, and provides to the *Client* details of the steps that the *Consultant* is taking to address the potential non-compliance and prevent the same from recurring, together with any mitigating factors that it considers relevant.

ZM24: Extending the *service*

ZM24.1 The *Client* may, with the agreement of the *Consultant*, increase the period during which the Consultant Provides the Services for a period of one year. The total period during which the Consultant Provides the Service does not extend beyond 30 October 2022.

ZM24.2 The *Client* notifies the *Consultant* in writing not less than 12 months before the end of the *completion date* whether or not it proposes to increase the period. If the *Client* proposes to increase the period, the *Consultant* notifies the *Client* in writing within 4 weeks of the *Client's* notification whether or not it accepts the proposal.

SCHEDULE 2 – DATA PROTECTION SCHEDULE

1. Definitions

Data Controller: any person who falls under the definition of "controller" in the GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Consultant under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Processor: any person who falls under the definition of "processor" in the GDPR.

Data Protection Legislation:

(a) the GDPR, and any other applicable Law governing the processing of Personal Data and privacy and any subordinate or related legislation;

(b) any guidance, codes of practice or instruction issued by the ICO (or any other relevant regulatory supervisory authority from time to time;

(c) any replacement to, addition to, or amendment of, any of the foregoing including any national law or regulations constituting a replacement or successor data protection regime to that governed by GDPR; and

(d) any other applicable Law governing the processing of Personal Data and privacy which may come into force from time to time.

Data Protection Officer: the role as defined under Chapter IV, Section 4 of the GDPR.

Data Subject: an individual who falls under the definition of "data subject" in the GDPR.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

GDPR: Regulation (EU) 2016/679 of the European Parliament and the Client of 27 April 2016, otherwise known as the General Data Protection Regulation, the requirements of which will be applicable from 25 May 2018.

Law: any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforcement right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements of any regulatory body with which the Consultant or Client is bound to comply.

Personal Data: any information which falls within the definition of "personal data" under the GDPR [supplied by the Client to the Consultant or lawfully obtained by the Consultant during the performance of the Services.

Personal Data Breach: a breach of security that affects the confidentiality, integrity or availability of Personal Data from the accidental or unlawful loss, destruction, corruption, alteration, unauthorised disclosure of, or access to, Personal Data.

2. Data protection

2.1. The *Client* and the *Consultant* acknowledge that for the purpose of the Data Protection Legislation, the *Client* is and will remain the Data Controller and the *Consultant* is the Data Processor in respect of the processing of Personal Data under this Agreement. The Appendix to this Schedule sets out the scope, nature and purpose of the processing by the Consultant, the duration of the processing and the types of Personal Data and categories of Data Subject.

2.2. The *Consultant* shall immediately inform the *Client* if, in its opinion, an instruction infringes Data Protection Legislation.

2.3. The *Consultant* shall (and shall procure that any of its staff involved in the processing of Personal Data shall) comply with its obligations under the Data Protection Legislation which arise in connection with this Agreement.

2.4. Notwithstanding the general obligation in paragraph 2.3, where the *Consultant* is processing Personal Data as a Data Processor for the *Client*:

2.4.1. The *Consultant* shall only process the Personal Data in accordance with this Agreement, and in particular the Appendix to this Schedule, and on documented instructions from the *Client*, unless the *Consultant* is required to do otherwise by Law. If it is so required the *Consultant* shall promptly notify the *Client* before processing the Personal Data unless prohibited by Law;

2.4.2. The *Consultant* shall ensure that persons who have access to and/or process the Personal Data:

2.4.2.1. have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.4.2.2. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the *Client*, or as otherwise permitted by this Agreement;

2.4.2.3. have undergone adequate training in the use, care, protection and handling of Personal Data and training is kept up-to-date; and

2.4.2.4. are aware of and comply with the *Consultant's* duties under this paragraph 2

2.4.3. Taking into account the nature of the data to be protected, the harm that might result from a Data Loss Event, the state of technological development and the cost of implementation the *Consultant* shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

2.4.3.1. The pseudonymisation and encryption of Personal Data;

2.4.3.2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

2.4.3.3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

2.4.3.4. A process of regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.4.4. In assessing the appropriate level of security referred to in paragraph 2.4.3 above, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

2.5. The *Consultant* shall not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the *Client* has been obtained and the following conditions are fulfilled:

2.5.1. The *Consultant* or the *Client* has provided appropriate safeguards in relation to such transfer;

2.5.2. The Data Subject has enforceable rights and effective legal remedies;

2.5.3. The *Consultant* complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

2.5.4. The *Consultant* complies with reasonable instructions notified to it in advance by the *Client* with respect to the processing of the Personal Data.

2.6. Subject to paragraph 2.7 the *Consultant* shall notify the *Client* immediately if it:

2.6.1. Receives a Data Subject Access Request (or purported Data Subject Access Request);

2.6.2. Receives a request to rectify, block or erase any Personal Data;

2.6.3. Receives any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation;

2.6.4. Receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

2.6.5. Of becoming aware of a Personal Data breach;

2.6.6. Receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

2.6.7. Becomes aware of a Data Loss Event.

2.7. The *Consultant's* obligation to notify under paragraph 2.6 shall include the provision of further information to the *Client* in phases, as details become available.

2.8. Taking into account the nature of the processing, the *Consultant* shall provide the *Client* with full assistance and co-operation in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 2.6 (and insofar as possible within the timescales reasonably required by the *Client* including by promptly providing:

2.8.1. The *Client* with full details and copies of the complaint, communication or request;

2.8.2. Such assistance as is reasonably requested by the *Client* to enable the *Client* to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

2.8.3. The *Client*, at its request, with any Personal Data it holds in relation to a Data Subject;

2.8.3.1. Assistance as requested by the *Client* following any Data Loss Event;

2.8.3.2. Assistance as requested by the *Client* with respect to any request from the Information Commissioner's Office, or any consultation by the *Client* with the Information Commissioner's Office.

2.9. The *Consultant* shall maintain complete and accurate records and information to demonstrate compliance with this paragraph 2 and allow for audits, including inspections, conducted by the *Client* or another auditor mandated by the *Client*.

2.10. The *Client* shall designate a Data Protection Officer if required by the Data Protection Legislation.

2.11. The *Client* does not consent to the *Consultant* appointing any third party processor of Personal Data under this Agreement.

2.12. At the choice of the *Client*, the *Consultant* shall delete or return all the Personal Data to the *Client* at the end of Term and delete existing copies unless applicable Law requires storage of the Personal Data.

2.13. The *Consultant* shall indemnify the *Client* in full in respect of all claims, demands, losses and liabilities of the *Client* which arise from any breach of the provisions of this paragraph 2.

APPENDIX TO DATA PROTECTION SCHEDULE

Notes:

1. The *Consultant* shall comply with any further written instructions with respect to processing by the *Client*.

2. Any such further instructions shall be incorporated hereinto.

Description	Details
Subject matter of the processing	*This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*1 October 2019 to 30 September 2022 (or to 30 September 2023 if the contract is extended by one year) [Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include, by way of examples only: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state	*[Describe how long the data will be retained for, how it be returned or destroyed]*

law to preserve that type of data	