This **Agreement governing the obligations imposed by the Regulation (EU) 2016/679** made on [ ]

Between:

(1) **The GBC Pension Scheme**, registered in and established under the laws of United Kingdom whose registered address is at Chelworth Industrial Estate, Cricklade, Swindon, SN6 6HQ (the "Controller"); and

(2) **03110950 Ltd t/a Cranfords** incorporated in and established under the laws of Gibraltar whose registered office is at 48 Chorley New Road, Bolton, BL1 4AP(The "Processor")

Contents

Background

1. **Definitions and Interpretation**
2. **Consideration**
3. **Subject matter and duration of the processing**
4. **Nature and purpose of the processing**
5. **The type and categories of data being processed**
6. **The obligations and rights of the Data Controller**
7. **The obligations of the Data Processor**
8. **Conditions for consent**
9. **Subject Access Requests**
10. **Records of Processing Activities**
11. **Data Protection Impact Assessments**
12. **Appointing a DPO**
13. **Confidentiality**
14. **Notification of personal Data Breach**
15. **Sub-Contracting**
16. **Term and Termination**
17. **Governing law**

BACKGROUND

(A) The Controller determines the purpose and means of the processing of personal data as detailed in the Administration Agreement signed between the Scheme and the Scheme Administrator.

(B) The Processor processes personal data on behalf of the Controller as detailed in the Administration Agreement signed between the Scheme and the Scheme Administrator and as required by the Regulatory Authorities (HMRC and TPR).

(C) The Controller has engaged the services of the Processor to process personal data on its behalf.

(D) Article 28 of the Regulation 2016/679 provides that the Controller uses only Processors that provide sufficient guarantees to implement appropriate and necessary measures of processing that meet the requirements of the Regulation and ensure the protection of the rights of the data subjects.

(E) Article 28 (a) of the Regulation 2016/679 provides that where processing is carried out by a processor on behalf of a controller, such processing is governed by a contract binding the processor to the controller stipulating that the processor shall act only on instructions from the controller, from the appropriate industry regulators and ensures that appropriate technical and organisational measures required under the governing law are implemented by the processor to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing.

(F) In compliance with the above-mentioned provisions of the Regulation 2016/679 the Controller and Processor wish to enter into this security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"**GDPR**" (General Data Protection Regulation) shall mean Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"national law" shall mean the law of the Member State in which the Processor is established;

"personal information" shall mean any information relating to an identifiable natural person ('data subject'); an identifiable person is one that can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic cultural or social identity of that person;

"processing personal data" shall mean obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data. This includes data manipulation of forms of organising and retrieving data; adaptation, alteration, or modification of the data; use of the information or data; transmitting the data and making data available; destroying, blocking, or erasing data.

"sub-contract" and "sub-contracting" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted;

"technical and organisational security measures" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing; and

"DPIA" (Data Protection Impact Assessment) shall mean an assessment aimed at identifying risks to personal information.

"DPO" Data Protection officer.

2. CONSIDERATION

2.1 in consideration to the Controller engaging the services if the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed under this Agreement.

3. SUBJECT MATTER AND DURATION OF THE PROCESSING

3.1 The Controller provides the Processor only the data that is necessary for the carrying out the duties listed within the Administration Agreement and subsequent duties that arise from that agreement in relation to governing legislation and regulatory requirements. This data includes Trustee personal information and in some cases may include special categories data, such as details about the Trustee's health and other sensitive data. Art. 9 GDPR.

3.2 The Processor will ensure that the data is used to carry out contractual duties in relation to administration of the Pension Scheme in the manner specified within the Administration agreement and the GDPR Agreement and is kept in a secure manner accessible by staff members authorised to process the data.

3.3 In the event of special category data is processed in order to carry out the contractual and legal obligations by the Processor, specific consent is requested from the data subject prior processing and necessary measures are implemented in order to keep the data safe, including restricted access to such data, based on staff clearance levels.

3.4 The Controller and the Processor have the obligation to keep the data for the period of the contract and a further six years from the termination of the contract. In the event of Agreement where special categories data is being processed, depending on the specific nature of the special categories data, this period will be longer and can be up to 10 years after the data subject's death.

4. NATURE AND PURPOSE OF THE PROCESSING

4.1 The data processing is for the purpose of carrying out the duties of the Scheme Administrator; and/or practitioner as detailed in the Administration Agreement and the Trust Deed and Scheme Rules and in accordance to the applicable laws; which include sharing elements of data with the HMRC and The Pensions Regulator.

5. THE TYPE AND CATEGORIES OF PERSONAL DATA BEING PROCESSED

5.1 The type and categories of data being processed in fulfilling the obligations of the Scheme Administrator and/or Processor are

a) Identification details of the scheme members - name, address, date of birth and national insurance number.
b) Proof of identification with a photo ID and proof of address.

c) Earnings, savings, inheritance and tax information relating to the scheme members.
d) Personal details relating to dependents, marriages, divorces and deaths.

5.2 The processor does not carry out automated profiling of clients.

6. THE OBLIGATIONS AND RIGHTS OF THE DATA CONTROLLER

6.1 The Data Controller determines the purpose and the manner of the data processing as detailed in the Trust Deed and Scheme Rules and Administration Agreement and the Scheme GDPR Agreement.

6.2 The Data Controller exercises the overall control over the data processing activities.

6.3 The Data Controller holds final accountability in the event of a Data Breach or for being found to be non-compliant with the GDPR.

6.4 The Data Controller is responsible for:

a) Complying with the principles;
b) Honouring Data Subjects rights;
c) Ensuring the processing of the data is lawful;
d) Appointing a DPO;
e) Demonstrating compliance;
f) Managing a Joint Controller relationships;
g) Managing Data Processors;
h) Record keeping;
i) Co-operation with the Supervisory Authorities;
j) Keeping personal information secure;
k) Ensuring transparency about Data Breaches;
l) Ensuring the Data Subject is notified with the relevant safeguards that are in place if the data is transferred into a third country.

7. THE OBLIGATIONS OF THE DATA PROCESSOR

7.1 The Data Processor will perform processing defined by the Data Controller and legal requirements to carry out the tasks as required by the Trust Deed and Scheme Rules, the Administration Agreement and the Scheme GDPR Agreement.

7.2 The Data Processor may decide within the terms of the Agreements with the Data Controller what IT systems and methods are required to collect and store the data; the security methods it applies to safeguard the data; the means used to transfer the data from one organisation to another; the means to retrieve personal data; the method of ensuring

retention schedule is adhered to; the method of data minimisation process it applies; and the means it uses to delete the data at the end of the required period.

7.3 The Data Processor is responsible for:

a) Complying with the principles;
b) Honouring Data Subjects rights;
c) Appointing a DPO if necessary;
d) Performing only the processing as per agreements with the Data Controller;
e) Updating the Data Controller;
f) Sub-Processor appointment and agreements;
g) Keeping personal information confidential;
h) Record keeping;
i) Co-operating with the Supervisory Authorities;
j) Keeping data secure;
k) Notifying the Data Controller of Data Breaches.

8. CONDITIONS FOR CONSENT

8.1 The Legal basis of the processing under this Agreement is the Administration Agreement between the Data Controller and the Data Processor; however there are specific areas that require a clear indication of consent, from the Trustee(s) who are the Data Subject(s) under this Agreement, found on the signature page of this Agreement.

9. SUBJECT ACCESS REQUEST

9.1 The Data Processor must respond to Subject Access Requests from the Data Subjects within one month and provide information about:

a) the purpose of processing;
b) the categories of personal data held;
c) the recipients to whom the personal data has been disclosed;
d) the period for which the personal data will be kept and the criteria used in determining the period;
e) notification that the Data Subject has the right to request rectification of data kept;
f) notification that the Data Subject has the right to place a restriction to the processing of data subject to lawful restrictions;
g) notification that the Data Subject has the right for the data to be deleted, subject to any lawful restrictions;
h) the source of data, in the event that the data was not collected from the Data Subject.

9.2 The Information requested must be provided in a simple and easily accessible format.

9.3 If further copies are requested, an administrative cost can be applied to the request to cover the cost of producing such copies.

9.4 The Subject Access Request must not have a negative effect on the rights and freedoms of others.

10. RECORDS OF PROCESSING ACTIVITIES

10.1 Both the Data Controller and Data processor shall maintain a record of processing activities under its responsibility.

The Controller and Processor need to keep the following records:

a) The details of the Controller, Processor, Representatives and the DPO;
b) The processing activities carried out;
c) Information relating to cross-border data transfers;
d) A description of security measures put in place to protect the data.

10.2 The records must be written and in electronic format where possible.

10.3 The records must be available for audit by the supervisory authority on request.

11. DATA PROTECTION IMPACT ASSESSMENTS

11.1 The Data Processor ensures that in the event of implementation of a new system or process that may have and adverse affect or carry a risk to personal data, a DPIA is carried out and a record of it is provided to the Data Controller.

12. APPOINTING A DPO

12.1 The UK Data Protection Bill 2018 Chapter 4. Chapter 69 puts further responsibilities on the UK based Data Controllers by requiring the appointment of a data protection officer as opposed to GDPR where the requirement is conditional.

12.2 The Data Protection officer is responsible for:

a) Providing information and advice in relation to GDPR processes and compliance;
b) Liaising with the Supervisory Authority;
c) Providing the Controller, Processor and their employees who are actively involved with processing the personal data with advice regarding how to implement and adhere to their obligations in the context of GDPR;

d) Monitor compliance with the GDPR, including raising awareness, assigning responsibilities and training staff involved with processing and related audits;
e) Provide advice in relation to DPIAs and monitor its performance pursuant to Art.33.

13. CONFIDENTIALITY

13.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, unless there is a prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

13.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

13.3 The obligations in clauses 13.1 and 13.2 above shall continue for a period specified in the Administration Agreement and for the time period required by law for the retention of the information subject to the nature of information held.

13.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

14. NOTIFYING OF PERSONAL DATA BREACH

14.1 Obligation to notify under GDPR:
a) The Data processor must notify the Data Controller;
b) The Data Controller must notify the Supervisory Authority;
c) The Data Controller must make the Data Subjects aware of the breach.

14.2 The obligation to notify exists if:
a) The breach is likely to effect the rights and freedoms of data subjects;
b) There is a reputational risk, financial implication, loss of confidentiality, risk of discrimination, social and economic disadvantage that may fall on the data subject as a result of the breach;

14.3 Data breaches must be notified within 72 hours of the breach being discovered by downloading a form from the ICO website and sending it back to them.

14.4 Data Controller shall keep record of all data breaches containing the details and effects of the breach and action taken to rectify it.

15. SUB-CONTRACTING

15.1 The Processor shall be able to undertake necessary sub-contracting in order to carry out its contractual duties to the relevant standard without the written consent from the Controller.

15.2 If sub-contractors are used, the same rules shall apply to the sub-processor as found in this Agreement.

16. TERM AND TERMINATION

16.1 This Agreement shall continue in full force and effect for as long as the Processor is processing personal data on behalf of the Controller.

16.2 Within 60 days following termination of this Agreement the Processor shall, at the direction of the Controller:

a) comply with any other arrangement made between the parties concerning the return or destruction of the data, or
b) return all personal data passed to the Processor by the Controller for processing, or
c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

17. GOVERNING LAW

17.1 This Agreement shall be governed by and construed in accordance with the laws of England and Wales.

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of The GBC Pension Scheme

(Authorised signatory)

(Print name and title)

SIGNED on behalf of Cranfords

(Authorised signatory)

(Print name and title)