PERSONAL DATA PROCESSING AGREEMENT

This Data Processing Agreement is made this …… day of ……... 20…….. and forms an integral part of the Contractor's Terms of Service (hereinafter referred to as Principal Agreement) between **Lincolnshire Co-operative Limited** (hereinafter referred to as "Controller" or "Society" and [CONTRACTOR'S COMPANY'S NAME] (hereinafter referred to as "Processor" or the "Contractor").

For the purposes of this agreement (the "Agreement"), the Controller and the Processor are hereinafter individually referred to as a "Party" and collectively as the "Parties".

WHEREAS

a) The Controller and Processor have entered into an *Agreement* for the provision of [INSERT THE NATURE OF THE SERVICE] services by the Processor to Controller.

b) Based on the above, certain Personal Data and information relating to an identified or identifiable natural person ('Data Subject') collected by the Processor on behalf of the Controller.

c) These Personal Data will be processed for purposes of providing the Services set out under the Principal Agreement.

d) This Agreement is intended to govern the transfer and processing of Personal Data of the Data Subjects from the Processor to the Controller in line with the General Data Protection Regulation, (GDPR) 2016/679) **("EU GDPR") and (UK GDPR)** and the United Kingdom ("UK") Data Protection Act 2018 and any other applicable data protection or privacy-related legislation and\or regulations governing Personal Data in the jurisdiction in which the Services are being provided.

The Parties hereby agree to the terms as reproduced below:

1. Definitions

"**Agreement**" means this Third-Party Data Processing Agreement and its Appendix

"Controller" means Lincolnshire Co-operative Limited.

"Instruction" means any written instruction from the Controller to the Processor as regards specific action regarding the personal data disclosed to the Processor.

"GDPR" means General Data Protection Regulation, (GDPR) 2016/679).

"Principal Agreement" means the *[insert name of agreement]*

"**Processor**" means **[Insert name of third-party processor]**

"**Services**" means the services the Processor provides to the Controller under the Principal Agreement.

"Sub Processor'' means any third-party processor appointed by and on behalf of the Processor in connection with this Agreement.

"Standard Contractual Clauses (SCCs)'' means the ICO's international Data Transfer Addendum to EU Commission Standard Contractual Clauses ("Addendum") and Module 2 of the European Commission's Standard Contractual Clauses for transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in Annex to Commission Implementing Decision (EU) 2016/679 as set out to Annex to Commission implementing Decision (EU) 2021/914 ("EU SCCs").

Data, Data Subject, Data Transfer, Personal Data, Personal Data Breach, Processing, Third Party, Supervisory Authority shall have the meaning attached to them in the GDPR.

2. Obligations of Both Parties

2.1 Each Party shall comply with Data Protection Laws (as amended or re-enacted from time to time) to the extent it is directly applicable in receipt or delivery of Services under the applicable agreement and Terms & Conditions.

2.2 Each Party shall comply with their obligations as defined in this Data Protection Agreement (DPA).

2.3 The DPA is subject to the terms of the Agreement and in any event of any conflict between any terms of Agreement and this DPA, this DPA shall take priority. References to "Clauses" in this DPA are to clauses of this DPA unless specified otherwise.

2.4 Each Parties warrant in relation to Personal Data that it will (and will ensure that any of its staff and/or Sub processors will comply with the Data Protection Laws

2.5 The Parties acknowledge and agree that the Society is the Controller, and the Contractor is the Processor

3. Obligations of the Processor

3.1 The Processor shall ensure full compliance with the GDPR and other Data Protection Laws in processing the Personal Data disclosed by the Controller or collected on behalf of the Controller.

3.2 The Processor shall ensure that Personal Data is only processed and stored as necessary for the purpose(s) specified in the Principal Agreement, terms of this DPA, Schedule 1 & 2 and under Applicable Laws.

3.3 The Processor shall only process Personal Data in accordance with the Controller's Instruction.

3.4 The Processor shall maintain adequate physical, technical, and administrative security measures to safeguard and ensure the protection and security of all personal data transferred and disclosed to it by the Controller (including where relevant, Article 32 GDPR), from loss, misuse, unauthorized access, alteration accidental or unlawful destruction, unauthorized disclosure, or access. Such measures and safeguards may include but are not limited to the following:

- developing organizational policy for handling Personal Data.
- protecting systems from hackers.
- setting up firewalls.
- storing Personal Data securely with access only to specific authorized individuals.
- employing data encryption technologies.
- ensuring that Personal Data cannot be read, copied, modified, or deleted without a prior written consent of the Data Controller; and
- putting in place a proper data mapping system.

4. Confidentiality

4.1 The Processor will ensure that anyone who has access to the Personal Data disclosed by the Controller is subject to a duty of confidentiality by putting in place a confidentiality agreement or acceptable use policies. The undertaking to confidentiality shall continue after the termination of this Agreement.

4.2 The confidential information must not be disclosed to a third party except:

a) the prior written consent of the Controller has been sought and obtained.
b) the disclosure is required by law; or
c) the relevant information is already in the public domain.

5. Personal Data Breaches

5.1 All suspected, actual, threatened, or potential Data Breaches must be reported immediately it is identified by the Processor to the Controller without undue delay of its occurrence and with sufficient information to allow the Controller to meet any required obligation to report to the Regulator or inform the Data Subjects of the Personal Data Breach under the GDPR.

5.2 The Processor shall assist the Controller and take reasonable steps as are directed by the Controller, in the investigation and take steps to manage, mitigate and remediate the Personal Data Breach.

5.3 Examples of data privacy breaches include but are not limited to

a) transmission of Personal Data across borders without requisite consent or approvals.
b) loss or theft of data or equipment on which data is stored.
c) accidentally sharing data with someone who does not have a right to the information.
d) inappropriate access controls allowing unauthorized use.
e) equipment failure.
f) human error resulting in data being shared with someone who does not have a right to know; and
g) a hacking attacks.

6. Deletion and Return of Personal Data

6.1 On expiry or termination of this agreement, the Processor shall immediately cease to use client data and shall arrange for its safe return or destruction as shall be required by the Controller (unless European Union, Member States and/or UK Law requires storage of any personal data contained within the client data or an exemption under GDPR applies).

6.2 The Processor shall within 14 days of the cessation of the Principal Agreement provide written certification to Controller that it has complied with the provisions of this Clause 5.

7. Data Transfer to Foreign Jurisdiction

7.1 The Processor must not transfer, disclose, or authorize the transfer of Personal Data outside the UK without the prior written consent of the Controller.

7.2 To the extent that the performance of the Processor's obligations, and any supporting and/or ancillary activities, involves processing the Controller's client data, the Processor shall only carry out processing of the Controller's client data in accordance with the Controller's documented instructions , including where relevant for transfers of EEA resident Client Data outside the EEA or to an international organisation (unless the Processor is otherwise required to process client data by European Union, Member State and/or UK law to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement unless prohibited by that law on important grounds of public interest), and shall immediately inform the Controller if, in the Processor's opinion, any instruction given by the Controller to the Processor infringes privacy and data protection requirements;

7.3 Subject to the paragraphs below, if an EEA resident's personal data is to be processed outside of the EEA, the Processor agrees to provide and maintain appropriate safeguards as set out in Article 46 GDPR to lawfully transfer the personal data to a third country.

7.4 The above shall not apply if the processing of the personal data is carried out in a country that the European Commission has considered as offering an adequate level of protection.

7.5 Where the Controller has consented to such transfer and acknowledges and accepts that certain Data Suppliers engaged by the Processor in the provision of the products and services are in a country that the European Commission has not formally declared to have an adequate level of protection (Transfers based on adequacy decisions / Article 45(3) GDPR) and are not able to demonstrate appropriate safeguards (Transfer subject to adequate safeguards / Article 46 GDPR). In such circumstances this will be stated in the additional terms and the Controller acknowledges that prior to submitting client data to the Processor for processing it shall determine, and is solely liable for ensuring, that one of following exceptions set out in Article 49 GDPR applies:

(a) the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards.

(b) the transfer is necessary for the performance of a contract between the Data Subject and the Controller, or the implementation of pre-contractual measures taken at the Data Subject's request.

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person.

(d) the transfer is necessary for important reasons of public interest.
(e) the transfer is necessary for the establishment, exercise, or defence of legal claims.

(f) the transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent, or

(g) the transfer is made from a register which according to European Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by European Union or Member State law for consultation are fulfilled in the case.

7.6 If any Personal Data transfer between the Controller and the Processor requires execution of the SCCs to comply with Data Protection Laws, the Parties will ensure the execution of the SCCs and take all actions required to legitimate the transfer

7.7 Any transfer of Personal Data out of the EEA not in accordance with the provisions of the GDPR will be a breach of this Agreement and the Processor shall indemnify the Controller pursuant to the terms and conditions of this Agreement.

8. Subject Access Request

8.1 By virtue of the provisions of the GDPR, a Data Subject is entitled to request for confirmation of his/her information held by Controller through a subject access request. Where a Data Subject makes a Data Subject access request to the Processor, the Processor must without undue delay of the receipt of such request, notify the Controller of the request and request prior authorization of the Controller before responding.

8.2 Where the Controller makes a Data Subject access request to the Processor, the Processor shall within 3 working days take appropriate measures to respond to the request or meet any required obligations.

8.3 In addition to the rights of Data Subjects to request for access to Personal Data collected and stored by the Controller, the Data Subjects are also entitled to the following rights:

a) Request for objection or restriction of processing of Personal Data.
b) Right to information on your data collected and stored.
c) Right to object to automated decision making and profiling.
d) Right to withdraw consent at any time.
e) Right to request rectification and modification of your data which we keep.
f) Right to request for deletion of your data.
g) Right to request the movement of data from us to a Third Party; this is the right to the portability of data.

9. Audit

8.1 The Controller has the right to carry out an audit on the processing operations of the Processor to determine the compliance level of the Processor with this Agreement and the GDPR.

8.2 The Processor will be given 14 days' written notice in advance for the audit.

8.3 The Processor undertakes to give the Controller the necessary support and information during the audit or inspection to demonstrate the implementation of the organizational and technical measures put in place by the Processor.

8.4 The Processor shall notify the Controller of any inability to disclose such information, if precluded by any law or any other obligation under the GDPR.

8.5 Without prejudice to the right of the Controller to conduct an audit of the Processor's data processing activities, the Processor shall carry out its annual data protection and compliance audit in line with the provisions of the GDPR.

10. Sub-Processor(s)

9.1 The Processor shall not transfer or disclose the Personal Data to a third-party Sub Processor unless required and on the written authority of the Controller. This obligation shall continue even upon termination/cessation of this Agreement.

9.2 Where the Processor engages a Sub-Processor with the written authority of the Controller, the Processor will enter into a Data Protection Agreement with the Sub-Processor that imposes on the sub-processor the same obligations that apply to Processor under this Agreement.

9.3 The Processor shall ensure the Sub-Processor fulfills its data protection and processing obligations. Provided always that the Processor will remain liable to the Controller for all acts and or omissions of the Sub-Processors, as if those acts or omissions were that of the Processor.

11. Liability and Indemnity

The Processor shall indemnify the Controller and hold the Controller, its Directors, Employees, Officers, and its affiliates harmless from all damages, penalties, claims, costs (including without limitation attorney's costs) and any third-party claims arising from or in connection with any breach of the provisions of this Agreement or the provisions of the GDPR.

12. Severability

If any provision of this Agreement is declared by any judicial or other competent authority to be void or otherwise unenforceable, that provision shall be severed from this Agreement and the remaining provisions shall remain in force and effect.

IN WITNESS WHEREOF, the Parties have entered into this Agreement the day and year first above written.

Signed and Delivered by the within named Controller, **Lincolnshire Co-operative Limited.**

Signature:_____

Name: _____

Title: _____

Date: _____

Signed and Delivered by the within named Processor, **[INSERT CONTRACTOR's COMPANY'S NAME]**

Signature:_____

Name:_____

Title: _____

Date: _____

Schedule 1

This Schedule 1 forms part of the DPA and describes the processing and transfer of Controllers Personal Data by the Contractor with the Agreement

Description	Purpose
Individuals may include	[**Drafting note: select as appropriate** - employees, members, customers]
Categories of Personal Information	**Drafting note**: **select as appropriate** – Names, Emails, Job Title, IP addresses, other personal contact details, location data, purchase history, financial information (including payment information), business travel and expenses, age, gender, nationality, government ID numbers, information, personal interaction with LCL
Special Categories of Personal Information	**Drafting note**: **select as appropriate** – Ethnicity or Race, medical or health information, trade union affiliation, political affiliations, religion or philosophical beliefs or affiliations, information regarding criminal convictions, sexual orientation or sex life, genetic, genetic information, biometric data biological samples etc.
Frequency of Transfer	**Drafting note**: **select as appropriate - [Continuous or One-off]**
Purpose of Processing	
Duration of Processing	For the duration of the Agreement. Upon expiry or termination of the Agreement, the Supplier shall return or delete the Controller's Personal Data in accordance with Section 6.1 and 6.2 of the Agreement.

Schedule 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Schedule 2 forms part of the DPA and describes the minimum technical and organisational measures implemented by the Contractor to protect the Controller's Personal Data from Security Incidents:

Technical Measures	Description
Policies and Governance	
Encryption	
Anti-Intrusion Software	
Access Controls	
Availability and Back-up	
Selection of service providers or sub-processors	

Disposal of IT equipment	
Monitoring, Logging and Auditing	
Physical Security	

Schedule 3

LIST OF SUB-PROCESSORS

Schedule 3 forms part of the DPA. The list of sub-processors the supplier will engage and will be processing the personal data with LCL.

Third Party Name	Service Being Provided	Third Party Location