DATA SHARING AGREEMENT

between

City of Edinburgh Council

and

CHANGEWORKS RESOURCES FOR LIFE LIMITED

Contents

1. Definitions 3

2. Purpose 5

3. Responsibilities 5

4. General Obligations 6

5 Data Sharing 6

6 Access to Data and Rights of Data Subjects 7

7 Term and Termination 8

8 Review 8

9 Entire Agreement 9

10 Governing Law and Jurisdiction 9

11 Data Protection Principles 9

12 Technical Security Measures 10

13 Organisational Security Measures 10

14 Scottish Government Privacy Principles 11

15 Signatures 12

The Schedule 13

This Data Sharing Agreement ("**Agreement**") forms part of the Contract for Services between:

- **THE CITY OF EDINBURGH COUNCIL**, a local authority in terms of the Local Government etc (Scotland) Act 1994 having an office at Waverley Court Business Centre, 4 East Market Street, Edinburgh, EH8 8BG ("**the Council**") and
- CHANGEWORKS RESOURCES FOR LIFE LTD a company incorporated under the Companies Act (Company Number SCO103904) whose registered office is at 36 Newhaven Road, Edinburgh, EH6 5PY (**"Changeworks**")

together referred to as the "**Parties**", and separately as a "**Party**"

Background

Changeworks and the Council proposes to share information for the purpose(s) of:

- Providing an energy advice service to Council tenants

The information to be shared includes Personal Data as defined by the Data Protection Legislation.

It is agreed as follows:

1. Definitions

The following definitions apply:

Agreement: This Agreement which is a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

Consent Form: The form of words to gain consent provided to the relevant individuals in the form of the template in the Schedule.

Data Discloser: The Party transferring the Personal Data to the Data Receiver.

Data Receiver: The Party receiving the Personal Data from the Data Discloser.

Data Protection Legislation: Any law applicable relating to the processing, privacy and use of personal data, including, without limitation: (i) The Data Protection Act 2018 (the **DPA**); (ii) The UK General Data Protection Regulation (the **UK GDPR**) and/or any equivalent national laws or regulations; (iii) the Electronic Communications Data Protection Directive (2002/58/EC); (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and/or (v) any judicial or administrative implementation of any of the above, any guidance, guidelines, codes of practice, codes of conduct or approved certification mechanisms issued by the Information Commissioner's Office, or other regulatory or supervisory authority responsible for administering Data Protection Legislation.

Data Retention Period: The duration for which the Personal Data will be held. Organisational Data Retention policies describe the periodical review of the Personal Data held, which will be erased or anonymised it is no longer legitimately needed.

Data Subject: Any person whose personal data is being collected, held, or processed.

Data Type: The Personal Data described in the Schedule which relates to an identified or identifiable individual.

Disclosing Party: A Party which shares Personal Data, of which it is the Controller, with the other Party pursuant to this Agreement.

Effective Date: The date from which the project contract starts, as described in the Schedule.

Good Practice: That standard of skill, care, knowledge and foresight which would be reasonably and ordinarily expected of an experienced and responsible person carrying out the activity in question.

Personal Data: Information that relates to an identified or identifiable individual. Also referred to as "**Data**" in this agreement.

Principles: The Data Protection principles as set out in Clause 12 of this Agreement, as amended from time to time.

Privacy Notice: The document which informs individuals what their Data will be used for. Privacy Notices for each Project are consistent with the Project Purpose. They accurately reflect what happens to the Data and explain that the Data may be shared with the other Party to this Agreement.

Project(s): The Project(s), described in the Schedule, known as ***The Energy Advice Service***

Purpose: The reason for sharing Personal Data as described in the Schedule or as otherwise agreed between the Parties in writing from time to time.

Recipient Party: A Party who has received Data from the Disclosing Party pursuant to this Agreement and Processes that Data on behalf the Disclosing Party.

Schedule: The schedule at the end of this Agreement in eight (8) sections.

Security Breach: The accidental or unlawful destruction, loss, damage and/or alteration; unauthorised disclosure and/or access; and/or all other unauthorised or unlawful forms of processing of the Data.

Subject Access Request: has the same meaning as "Right of access by the data subject" in Chapter 3 of the DPA.

Term: shall mean the periods described in the Schedule.

Data Controller, Data Processor, Data Protection Impact Assessment, Special Category, Processing, and **appropriate technical and organisational measures** have the meanings given to them in the Data Protection Legislation.

2. Purpose

2.1 This Agreement is legally binding between the Parties and sets out the arrangements between the Parties in relation to the sharing of Data, in accordance with the provisions of the Data Protection Legislation and the provisions of the Human Rights Act 1998 which relate to personal privacy.

2.2 Both Parties are Data Controllers agreeing to share Personal Data as defined by Data Protection legislation.

2.3 The types of Data to be shared in terms of this Agreement are described, and solely for the Purposes in the Schedule.

3. Responsibilities

3.1 The Parties agree that they are Controllers in relation to all Data which they Process and share under this Agreement.

3.2 The Parties agree to adhere to the overarching requirements of the Data Protection Legislation, including the Principles.

3.3 Each Party shall act at all times in accordance with Good Practice and shall:

3.3.1 only Process the Data in compliance with the Data Protection Legislation and all other Applicable Law;

3.3.2 only Process the Data in a manner that is consistent with the Purpose and shall not use the Data for any other purpose;

3.3.3 adhere to the Data Retention Periods set out in the Schedule; and

3.3.4 otherwise adhere to the terms of this Agreement and its obligations under this agreement.

3.4 Each Party shall not:

3.4.1 sub-contract the performance of any of its obligations under this Agreement (or otherwise authorise any third party to Process the Data on its behalf);

3.4.2 sub-license the exercise of any of its rights under this Agreement; or

3.4.3 assign or otherwise transfer (as applicable) its rights and obligations under this Agreement, whether in whole or in part, without the prior written consent of the other Party.

3.5 Each Party shall ensure that they comply with their obligations as Controllers under the Data Protection Legislation and provide individuals with appropriate Privacy Notices in the form of the templates in the Schedule.

3.6 Where the Parties require to obtain individuals' consent to share the Data under this Agreement, the Parties hereby agree to use the form of words in the Schedule. The Parties will ensure that records of consent are maintained in accordance with the terms of the Data Protection Legislation

3.7 In line with the Data Protection Legislation and the Information Commissioner's Office advice, the Parties agree that it is not appropriate to ask for an individual's

consent in circumstances where the relevant professional staff acting in good faith have taken the view that the information will be released whether that consent has been given or not.

4. General Obligations

4.1 The Parties agree that they shall

4.1.1 ensure that access to the Data is limited to:

4.1.1.1 those employees who need access to the Data for the Purpose; and

4.1.1.2 in the case of any access by any employee, such part or parts of the Data as is strictly necessary for the performance of that employee's duties.

4.1.2 ensure that all employees:

4.1.2.1 are informed of the confidential nature of the Data;

4.1.2.2 have undertaken training in the laws relating to handling the Data;

4.1.2.3 are aware both of the duties of their employer and their own duties and obligations under such laws and this Agreement;

4.1.2.4 who have access to the Data are reliable; and

4.1.2.5 keep adequate records of all Processing of the Data that they carry out.

4.1.3 not share the Data with any other organisation unless they have obtained the other Party's prior written consent and the recipient organisation has entered into a written data sharing agreement in terms which are no less onerous than those contained in this Agreement.

5 Data Sharing

5.1 All disclosures of Data between the Parties shall be made as described in the Schedule.

5.2 In the event that any Data shared in terms of this Agreement contains Special Categories of Personal Data, the Parties shall comply with the Principles set out in Clause 12 of this Agreement.

5.3 Only the minimum amount of Data required for the Purpose will be shared between the Parties.

5.4 The Parties shall use reasonable endeavours to ensure that any Data shared in terms of this Agreement is up to date and accurate in all material respects.

5.5 The Disclosing Party shall, as soon as reasonably practicable, notify the Recipient Party of any updates or revisions to the Data.

5.6 As Controllers in terms of the Data Protection Legislation, each Party is responsible for the quality and accuracy of the Data that they record on their own management information systems. Identified discrepancies between what is on different Parties' management information systems will be discussed and resolved as part of ongoing partnership working. It is the responsibility of each Party to correct any recognised errors or inaccurate Data on their own management information system and notify the correction to the other Parties. This is to ensure that accurate Data is shared at all times.

5.7 The Parties hereby undertake to the other Party that they shall:

5.7.1 at all times have in place appropriate technical and organisational security measures to protect Data against a Security Breach, including (as a minimum) the respective measures relevant to and specified in Clause 13 of this Agreement; and

5.7.2 ensure that the technical and organisational measures referred to in Clause 14 ensure a level of security appropriate to the harm that might result from a Security Breach and the nature of the Data.

5.8 In the event of a Security Breach, each Party agrees to:

5.8.1 Notify the other Party as soon as reasonably practicable, and in any event no later than 48 hours after a Security breach has been identified, using the contact details listed in the Schedule.

5.8.2 Provide reasonable assistance to the other Party to resolve any issues occurring as a result of a Security Breach.

6 Access to Data and Rights of Data Subjects

6.1 Each Party shall assist the other Party within a reasonable timescale and as necessary with all requests from Data Subjects made under the Data Protection Legislation which may be received by either Party from a Data Subject.

6.2 Where none of the circumstances justifying the release of Personal Data under this Agreement applies in a particular case, or where a Data Subject has made a request under the Data Protection Legislation to the effect that one of the Parties is to delete, restrict the Processing of, or not to Process or further Process any Personal Data relating to that Data Subject, the Party or Parties entitled to see the Data in question shall ensure that it is not shared with the non-entitled Party.

6.3 Notwithstanding any other provision in this Agreement, the Parties acknowledge that the existence of this Agreement may be subject to requests made under the Freedom of Information (Scotland) Act 2002 ("**FOISA**") and/or the Environmental Information (Scotland) Regulations 2004 ("**EISRs**") and, subject to any applicable exemptions or exceptions as determined by the receiving Party of the FOISA or EISRs request, the content of this Agreement may be disclosed under FOISA or EISRs. Before disclosing any information relating to this Agreement in response to a request for information made under FOISA or EISRs, the Party in receipt of the FOISA or EISRs request shall, as soon as reasonably practicable after receipt, notify the other Party of such request.

6.4 The other Party may make representations as to whether, and on what basis, the information requested is covered by an exemption under FOISA or an exception under EISRs and thus should not be disclosed. The Party in receipt of the FOISA or EISRs request shall consider reasonably any representations made to it by the other Party before deciding whether to disclose the information requested. However, in all cases, it is for the Party in receipt of the FOISA or EISRs request alone to determine whether or not to disclose the information. Further, the Party in receipt of the FOISA or EISRs request shall not be obliged to notify the other Party where it has already decided that it does not intend to

disclose the information because FOISA or EISRs does not apply to the request or an exemption under FOISA or an exception under or EISRs can be applied. If the Party in receipt of the FOISA or EISRs request decides to disclose the information, it shall notify the other Party of this decision in advance of the disclosure being made.

7 Term and Termination

7.1 This Agreement shall continue in force for the Terms covered by the Schedule, starting from the Effective Date.

7.2 The Agreement shall automatically terminate on expiry of the Terms unless, following a review of the terms of the Agreement under Clause 7, the Parties agree to extend the Agreement.

7.3 Either Party may terminate this Agreement at any time on giving 30 days' notice in writing to the other Party.

7.4 The Parties agree that on expiry of the Term or earlier termination of this Agreement (howsoever caused), the Recipient Party shall, at the choice of the Disclosing Party, in respect of any data of which it is a Processor either:

7.4.1 Return all the Data transferred including any data storage media supplied to the Recipient Party and the copies thereof to the Disclosing Party within any timescales specified by the Disclosing Party and the Recipient Party warrants that it will guarantee the confidentiality of the Data transferred and will not actively Process the Data anymore; or

7.4.2 Destroy all the Data and certify to the Disclosing Party that it has done so within any timescales specified by the Disclosing Party.

7.5 If Applicable Law prevents the Recipient Party from returning or destroying all or part of the Data as in Clause 8.4, then the Recipient Party warrants that it will guarantee the ongoing confidentiality of the Data retained and will not actively Process the Data transferred anymore other than for the purpose to enable it to comply with such Applicable Law

7.6 In the event that this Agreement is terminated for any reason or where either Party withdraws from this Agreement, any duties of confidentiality imposed on the Parties in respect of this Agreement shall subsist indefinitely.

8 Review

8.1 This Agreement will be reviewed annually thereafter, but either Party can request that it be reviewed at any time providing reasonable cause can be shown.

8.2 Before any substantive changes are made the Agreement will be referred through the appropriate internal processes, including consultation with information governance colleagues.

8.3 The reviewers will consider whether:

8.3.1 The Agreement is achieving its Purpose

8.3.2 Information sharing is operating legally and smoothly

8.3.3 Processes require updating.

8.4 Both Parties must agree to any changes proposed as a result of the review before signing a refreshed agreement.

9 Entire Agreement

9.1 This Agreement constitutes the entire agreement between the Parties concerning its subject matter, namely the sharing of Personal Data, and supersedes and extinguishes all previous agreements, promises, assurances, understandings, warranties, or representations between them, whether written or oral, relating to its subject matter.

10 Governing Law and Jurisdiction

10.1 This Agreement and any dispute or claim arising out of it or in connection with it or its subject matter or formation shall be governed by and construed in accordance with Scottish law, and the courts of Scotland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

11 Data Protection Principles

11.1 Personal Data shall be Processed fairly and lawfully and in a transparent manner in relation to individuals. For Processing to be lawful under the Data Protection Legislation, a legal basis needs to be identified.

11.2 In the present Agreement, the legal basis for the Personal Data is that the Processing of the Data is consent.

11.3 Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner that is incompatible with the purposes described in the Schedule at the end of this Agreement.

11.4 Personal Data shall be adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed.

11.5 Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

11.6 The Parties are responsible for the quality and accuracy of the Data that they record on their own management information systems. If discrepancies are identified between Data on the Parties' management information systems, such discrepancies will be discussed and the Parties, as the case may be, shall take all reasonable endeavours to ensure that their respective management information systems are up to date. It is the responsibility of each Party to correct any recognised errors or inaccurate Data on their own management information system and inform the other Party of this.

11.7 Personal Data kept in a form that permits the identification of Data Subjects shall not be kept for longer than is necessary for the purposes for which the Personal Data are processed.

11.8 The Parties shall adhere to the Data Retention Periods set out in the Schedule at the end of this Agreement

11.9 Personal Data shall be processed in a manner that ensures appropriate security against unauthorised or unlawful processing and accidental loss or destruction of, or damage to, Personal Data, using appropriate technical or organisational measures.

11.10 The Parties are each responsible for the secure Processing of the Data that they receive and agree to take the technical and organisational security measures as set out in Clause 13 of this Agreement.

12 Technical Security Measures

12.1 The Parties shall have in place the following technical security measures:

- PCs and servers on which the Data is stored must be password protected;
- passwords are subject to minimum complexity requirements. This complexity requires that passwords contain at least 8 characters, consisting of alphabetical (at least 1 uppercase) and numeric characters.
- antivirus software is centrally managed and distributed with updates applied as they become available;
- a patch management policy and configuration management policy covering the ICT infrastructure that will store and process the Data;
- a firewall protects the corporate wide area network ("WAN") and provides VPN access from outside the WAN via domain authentication. Firewall firmware updates are technically assessed as they are released and are applied as required;
- security permissions are in place to restrict access to the Data based on security group memberships which are set according to each employee's role; and
- access into corporate applications and the Data within those applications is restricted by account permissions set according to the role of the employee.

13 Organisational Security Measures

13.1 The Parties shall have in place the following organisational security measures:

- an information technology policy set that includes an Information Security Policy which has been implemented with which all of its employees must comply;
- all Data must be protected in accordance with applicable legislation;
- access to the Changeworks building is by lock and key, access beyond the reception area is via keypad, and the server room is secured with lock and key. Access to the Council is by keycard and all electronic devices are password protected.
- laptops and other devices access central systems through a suitable secure gateway. Laptops must employ encrypted hard drives;
- data exchanged between devices is encrypted;

- access to files and folders is controlled via user authentication and permissions, according to the employee's role. Email is restricted by the user's account;
- backup data is encrypted;
- clear policies and procedures must be in place for reporting managing and resolving security breaches associated with the Data; and
- data exchanged is retained or disposed of in line with the agreed retention policy.

14 Scottish Government Privacy Principles

Digital: Using data effectively

Principle	How the requirement will be met
1. Proving Identity or Entitlement	Data Subjects do not access the Data themselves; this does not raise any issues.
2. Governance & Accountability	These factors are addressed as set out in this Agreement.
3. Risk Management	The need for a DPIA has been determined in line with the ICO, and if appropriate one has been completed.
4. Data and Data Sharing	This Agreement records retention policies and procedures, and also defines and controls the scope and nature of Data being shared. The Parties intend to retain the Data in their independent management information systems and there will be no centralised databases containing the Data. Matching is required to provide reliable matching of Data to the right individual.
5. Data use for research and statistics	These factors are addressed as set out in this Agreement.
6. Education and Engagement	The Parties will continue to ensure their employees are suitably trained and informed about data sharing, data security and privacy. The Parties will apply their standard procedures when handling requests from Data Subjects.

15 Signatures

15.1 By signing this agreement, the Parties accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself meet the requirements and Purpose of this agreement.

On behalf of the Council:

Signature of Authorised Signatory	[redacted]
Print Name and Role	Derek McGowan (Service Director for Housing and Homelessness)
Date	31 March 2023
Signature of Witness	[redacted]
Print Name and Role	[redacted]
Date	31 March 2023

On behalf of Changeworks:

Signature of Authorised Signatory	[redacted]
Print Name and Role	[redacted]
Date	16th February 2023
Signature of Witness	[redacted]
Print Name and Role	[redacted]
Date	16th February 2023

The Schedule

This is the Schedule in 8 Sections referred to in the foregoing agreement between the Council and Changeworks Resources for Life Ltd.

1.1 Term

The Term of the contract is 03 Feb 2022 – 02 Feb 2026.

1.2 Data Sets

The following Data Sets will be shared between Changeworks and the Council (subject to the provisions of Clause 2 of this Agreement) in relation to Council tenants.

- Name
- Address
- Phone Number
- Email address
- Date of birth
- Children living at home
- Issues to consider (free type box)
- Benefits
- Health/Criminal Status
- Ethnicity
- Health Conditions
- Income/debt information

1.3 Purpose

The agreed purposes for which the Data may be Processed are set out under “Background”.

1.4 Legal Basis

The legal basis for sharing the Data from Changeworks to the Council and Contractors is consent from the Data Subject.

The legal basis for sharing the Data from the Council to Changeworks is Public Task.

The legal basis for sharing Special category data is Explicit Consent from the Data Subject.

1.5 Retention Periods

The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the agreed purposes as outlined in Section 1.3 and the Background.

Data gathered and held by Changeworks will be retained for a period of 6 years. At this time, all data will be anonymised except for any legal requirements preventing the data being deleted.

1.6 Privacy Notice / Consent Form

Changeworks Privacy Policy: Legal and Privacy | Changeworks

Changeworks will collect, process and securely store the information you provide for six years, to allow us to:

- **Help you with your energy matters**
- **Find out what you thought of the service**
- **Prove to our funders and auditors that we are using our funding for its intended purposes**
- **Carry out research about energy advice matters**
- **Provide you with related information if it may help you in the future.**

Changeworks must report summarised and anonymous data and project results to our funders. In addition, auditors may require to see all information about the support you received, including any information you provided.

We won't share your information with anyone else, unless you have given us permission to do so for a specific purpose. Otherwise, only in exceptional circumstances where there is a legal duty, would we share your information with a third party.
You have the right to see any information held on request. Please contact us or view our website for more information on how we manage personal information.

1.7 Data Sharing Methods

Data will be shared via:

- Changeworks AWS referral portal
- Referral form (via Changeworks website)
- encrypted emails/documents
- Sharepoint sites

Special Category Data will be shared via:

- Changeworks AWS referral portal – free type box
- Referral form (via Changeworks website) – free type box
- Encrypted emails to warmth@changeworks.org.uk

1.8 Contacts

Communication and Notices about this Agreement should be sent to the details listed below for each of the Parties. Each Party shall notify the other Party in writing of any changes to these details.

Changeworks	
Contact Name	[redacted]
Contact Address	Changeworks 36 Newhaven Road Edinburgh EH6 5PY
Contact Email	[redacted]@changeworks.org.uk

The Council	
Contact Name	[redacted]
Contact Address	The City of Edinburgh Council, Waverley Court, 4 East Market Street, Edinburgh, EH8 8BG
Contact Email	[redacted]@edinburgh.gov.uk

Notification of any Security Breach, Freedom of Information request or Subject Access request involving the personal data shared as per this Agreement shall be sent to the contact details below, as well as the contacts listed above.

Changeworks	
Contact Name	[redacted]
Contact Email	dataprotection@changeworks.org.uk

The Council	
Contact Name	
Contact Address	The City of Edinburgh Council, Waverley Court, 4 East Market Street, Edinburgh, EH8 8BG
Contact Email	informationcompliance@edinburgh.gov.uk