Lets Keep Talking CIC Limited

Data Controller

Document Version 4.1

Data Audit: 23 October 2026

ICO REGISTRATION NO: ZB 601598

C O R P O R A T E
R E S P O N S I B I L I T Y:-

Dr SUZANNE CURTIS

Data Protection Manager

DATA PROTECTION MANAGEMENT SYSTEM

Online Privacy Notice

LETS KEEP TALKING CIC LIMITED

Registered Member of the GDPR Check & Verify Register



www.gdprcheckandverify.com

1 COMPANY CONTACT DETAILS

1.1 Lets Keep Talking CIC Limited 54 St James Street, Liverpool. L1 0AB hereinafter referred to as 'the Company', We, Us and Our.

1.2 Our email address is: suzi@letskeeptalking.co.uk

1.3 Our contact telephone number is: 0800 090 2470

1.4 We are a Data Controller under the provisions of the UK GDPR and the Data Protection Act 2018 and have registered with the UK Information Commissioners office:

ICO Registration Number: ZB 601598

2 Status of key personnel

2.1 We have designated **Dr Suzanne Curtis** as **Data Protection Manager** for the business.

2.2 Please direct any data protection queries to the email address above.

3 INTRODUCTION AND OVERVIEW

3.1 This Privacy Notice explains how we collect, use and protect personal data when you

a) visit our website

b) contact us

c) buy products or services from us

d) otherwise interact with us

3.2 We are committed to protecting your personal information and complying with UK data protection law.

3.3 Further internal policies and procedures support our compliance with UK data protection law.

4 SCOPE OF THIS PRIVACY NOTICE

4.1 This Privacy Notice applies to Personal Data we process when you visit or use our website. Further Privacy Policy statements and documents may apply offline and these are available, if relevant, on request.

4.2 We have described below the personal information we may gather about you, the purposes we will hold it for and the limited categories of people to whom we may disclose it.

5 THE PERSONAL DATA WE PROCESS

5.1 During your visit to our site, we will only collect personal information that you choose to provide. If, for example, you contact us with an enquiry or request us to provide you with further information.

5.2 Where you provide us with another person's data you must ensure you have the authority to do so.

5.3 Depending on how you interact with us, we may process:

a) identity data (e.g. name);

b) contact data (e.g. address, email, telephone number);

c) financial and transaction data;

d) technical and usage data relating to website use;

e) marketing and communications data;

f) employment or recruitment data (where applicable).

We may also process limited special category data where necessary and lawful to do so.

6 HOW WE USE PERSONAL DATA

6.1 We use personal data for purposes including:

a) responding to enquiries;

b) providing products or services;

c) managing contracts and business relationships;

d) communicating with individuals;

e) maintaining website functionality and security;

f) complying with legal obligations;

g) protecting our business, staff, customers, and visitors.

h) using approved Artificial Intelligence (AI) technologies to support research, document preparation, analysis, administrative efficiency and service delivery, subject to appropriate human oversight and data protection safeguards.

7 LAWFUL BASES

7.1 We process personal data under one or more of the following lawful bases:

a) consent;

b) contract;

c) legal obligation;

d) legitimate interests;

e) vital interests;

f) public task (only if applicable).

7.2 Where we rely on legitimate interests, we carry out appropriate assessments and safeguards.

7.3 Further information regarding legitimate interests processing is available in the ANNEX to this document.

8 MARKETING COMMUNICATIONS

8.1 We may send Marketing communications where permitted by law including where:

a) Consent has been provided; or

b) Where the 'Soft opt in' provisions apply

8.2 Individuals may opt out of marketing communications at any time.

9 DATA SHARING

9.1 We may share personal data with:

a) service providers and data processors;

b) professional advisers;

c) regulatory, legal, or public authorities where required;

d) IT and communication providers.

9.2 We only share personal data where necessary and appropriate safeguards are in place.

10 INTERNATIONAL TRANSFERS

10.1 Where personal data is transferred outside the United Kingdom, we will ensure that appropriate safeguards are in place in accordance with UK data protection law.

10.2 Under UK data protection law, personal data may only be transferred outside the UK where one of the following applies:

(a) The destination country or organisation is subject to a UK adequacy regulation; or

(b) Appropriate safeguards are in place;

(c) A UK International Data Transfer Agreement (IDTA)

(d) An addendum to UK SCCs; or

(e) A limited statutory exception applies.

10.3 The Main Establishment for all of our Data Processing is the UK.

10.4 The competent supervisory authority is the UK Information Commissioner's Office (ICO). whose address is 4th Floor, No.3 Circle Square, 5 Hawkshaw Street, Manchester M1 7BL.

11 Personal Data under our control

11.1 The categories of personal data processing described in this section form part of the Company's Record of Processing Activities (ROPA) maintained in accordance with Article 30 UK GDPR and assigned a unique reference.

11.2 References to data processors are to individuals and organisations who have responsibility to us under a written data processing agreement compliant with Article 28 UK GDPR

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing	ROPA REF
Prospective and existing Clients providing their personal information either Online or Offline including Social Media, telephone and by written means to ourselves or third parties to request information regarding our available products and services	**Consent**	Identity Data Marketing Data Communications Data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.	RR-05
Clients providing their information for the purposes of contracting with us for goods and services. We process this Personal Data to provide relevant advice, to manage and administer our business relationships and communicate with clients, their employees and representatives, to manage billing and payments and to keep records.	**Contract**	Identity Data Financial Data Transaction Data Marketing Data Communications Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.	RR-05

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing	
Personal data provided because the Data Subject may be interested in working with us or learning more about working with us.	**Consent**	Identity Data	Time to consider request. Maximum of 12 months; or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.	RR-06
Online or Offline face to face meetings with people who provide their personal data to us for the purposes of later contact regarding products and services provided by us.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.	RR-05
Suppliers of products and services to us who provide information of themselves or individuals who assist them to provide us with products and services on their behalf.	**Contract**	Identity data Transaction Data	Duration of Contract Plus Seven Years	Data is shared with our Data Processors and our professional advisors including IT, Accounts and Legal where necessary.	RR-08
Personal Data of prospective customers provided by third parties for future contact by us regarding our products and services.	**Consent**	Identity data	Maximum of 12 months. Or Until Consent is withdrawn whichever comes first.	Data is only shared with our authorised Data Processors.	RR-07

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing	ROPA REF
Suppliers of software who manage data via End User Service Agreements (EUSAs).	**Contract**	Identity Data Transaction Data Technical Data	Duration of Contract Plus Seven Years	Data is only shared with our authorised Data Processors.	RR-08
Employees who provide their personal information for the purposes of working with us.	**Contract** **Legal Obligation** **Art.6 lawful basis** **Art.9 Condition (Employment)**	Special Category Data Identity Data Technical Data	Duration of Contract Plus Seven Years Any Other Legal Requirements	Data is shared with our Data Processors and our professional advisors including HMRC, IT, Accounts and Legal where necessary.	RR-06
Information collected through the use of Website Cookies	**Consent**	Identity Data Marketing Data Communications Data Transaction Data Technical Data	Varies depending on the Consent given and type of Cookie based on information provided to users.	Data is only shared with our authorised Data Processors and professional advisers as necessary	RR-09
Personal Data of individuals who make complaints under the DUAA 2025	**Legal Obligation**	Identity Data Technical Data	6 Years	Data is shared with our Data Processors our professional advisors and public bodies as necessary.	RR-10
People identified via proprietary Video Conference software	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists, the client objects or within 3 months if recorded whichever occurs first	Data is only shared with our authorised Data Processors	RR-02

Personal Data	Lawful Base(s)	Types of Data	Retention Period	Data Sharing	ROPA REF
People identified via proprietary Video Conference software	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists, the client objects or within 3 months if recorded whichever occurs first	Data is only shared with our authorised Data Processors	RR-02
People identified through our Dashcam Equipment	**Legitimate Interests**	Identity Data	Until Legitimate Interest no longer exists, the client objects or within 3 months if recorded whichever occurs first	Data is only shared with our authorised Data Processors	RR-04
Use of Artificial Intelligence where personal data is included	**Legitimate Interests**	Identity Data Marketing Data Communications Data Transaction Data Technical Data	Until Legitimate Interest no longer exists, or the client objects	Data is only shared with our authorised Data Processors and agents such as senior staff	RR-11 RR-12

12 DATA RETENTION

12.1 We retain personal data only for as long as necessary for the purposes for which it was collected, including legal, regulatory, accounting, or operational requirements.

12.2 Further information regarding retention periods is available on request.

13 DATA SECURITY

13.1 We use appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, or disclosure.

14 YOUR RIGHTS

14.1 Under UK data protection law, individuals have rights including:

a) the right to be informed;

b) the right of access;

c) the right to rectification;

d) the right to erasure;

e) the right to restrict processing;

f) the right to object;

g) the right to data portability;

h) rights relating to automated decision-making.

13.2 Requests relating to personal data rights may be made using the contact details above.

15 AUTOMATED DECISION MAKING

15.1 We do not carry out solely automated decision-making producing legal or similarly significant effects on individuals

15.2 We may use Artificial Intelligence (AI) technologies to assist staff with research, document preparation, analysis and administrative processes.

15.3 AI is used as a support tool and does not replace human decision-making. We do not carry out solely automated decision-making producing legal or similarly significant effects on individuals.

16 CHILDREN AND SAFEGUARDING

16.1 We recognise that personal data relating to children and safeguarding matters requires additional protection.

16.2 Where we process such data, we do so lawfully, proportionately, and with appropriate safeguards.

16.3 We will not knowingly collect information from persons under 13 years of age without their parent's or guardian's consent.

16.4 There is nothing on our Website which could be damaging to children who view the pages or the pictures.

17 COOKIES

17.1 Our website may use cookies and similar technologies.

What Are Cookies

17.2 Cookies are small text files that are placed on a user’s device when they visit a website. They are widely used to make websites work efficiently, improve user experience, and provide information to website operators.

17.3 Cookies may be:

a) Session cookies, which expire when the browser is closed; or

b) Persistent cookies, which remain on the device for a set period or until deleted.

How We Use Cookies

17.4 We use cookies to:

a) Ensure the website functions correctly

b) Maintain security and prevent fraud

c) Remember user preferences

d) Understand how the website is used, in order to improve performance and content

17.5 Cookies may be set by us ("first-party cookies") or by third parties providing services on our behalf ("third-party cookies").

Managing Cookie Preferences

17.6 Users can manage or withdraw their cookie preferences at any time by:

a) Using the cookie settings tool available on the website; and/or

b) Adjusting browser settings to block or delete cookies

Please note that blocking certain cookies may affect website functionality.

18 BUSINESS SALE OR TRANSFER OF OWNERSHIP

18.1 In the event our business, or part of it, is taken over, bought or merged with another business If our business is sold or reorganised, personal data may be transferred as part of that process, subject to appropriate safeguards.

19 COMPLAINTS

19.1 If you have concerns about how we have handled your personal data, we encourage you to contact our Data Protection Manager in the first instance using the contact details provided in this Privacy Notice.

19.2 We will investigate your complaint fairly, promptly and in accordance with our **Data Protection Complaints Procedure.**

19.3 If you remain dissatisfied after we have responded, you have the right to complain to the Information Commissioner's Office (ICO). Their Website is at: www.ico.org.uk

20 CHANGES TO THIS PRIVACY NOTICE

20.1 This Privacy Notice may be updated from time to time to reflect changes in law, guidance from the Information Commissioner's Office (ICO), or changes to our use of cookies.

20.2 The latest version will always be available on our website.

20.3 We may also update this Privacy Notice to reflect changes in our business activities or in applicable data protection law.

20.4 We reserve the right to make changes to this Data Protection and Privacy Policy, it is your responsibility to revisit this page from time to time to re-read this policy including any and each time you visit our website.

20.5 Any revised terms shall take effect as at the date of posting.

20.6 If you don’t find your concern addressed here, feel free to contact us by e-mailing our Data Protection Manager at the contact details given above.

ANNEX A – LEGITIMATE INTERESTS ASSESSMENTS (LIAs)

This Annex forms part of our Data Protection Management System (DPMS) and contains all current Legitimate Interests Assessments we rely upon.

Each LIA is approved by the Data Protection Manager and is reviewed annually.

LIA-01 – SOFT OPT IN

NOT USED

LIA-02 – VIDEO CONFERENCING

1. Processing Description
We use third-party video conferencing platforms to facilitate communication between staff, clergy, and stakeholders. In some cases, meetings may be recorded.

2. Purpose Test
Processing is necessary to:

- facilitate efficient communication across geographically dispersed participants;
- support operational and administrative activities;
- reduce the need for travel.

These are legitimate organisational interests.

3. Necessity Test
The Company considers that:

- video conferencing is the only practical method for real-time multi-party communication with visual content;
- alternative methods (e.g. telephone) are insufficient where visual information is required;
- use of such platforms is standard and expected in modern organisational operations.

4. Balancing Test

Nature of Data
Audio, video, and limited identifying information.

Reasonable Expectations
Participants would reasonably expect data processing when joining video calls.

Impact
Limited, as:

- recording is not routine;
- participants are informed where recording occurs;
- alternative participation (e.g. audio-only) may be offered where appropriate.

Risks to individuals
The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards
The Company applies the following safeguards to mitigate identified risks:

- platform security settings configured;
- access controls applied;
- recordings retained only where necessary;
- data handled in accordance with Company policies.
- Access to data is restricted to authorised personnel;
- data is stored securely and protected by appropriate technical measures;
- retention periods are limited;
- staff are trained in data protection requirements;
- policies and procedures govern the use of the data.

These measures reduce the likelihood and impact of identified risks.

5. Proportionality (DUAA)
Processing is targeted, limited, and proportionate to its purpose. No less intrusive method would achieve equivalent outcomes.

6. Conclusion
The Company has determined that processing is necessary, proportionate, and does not override the rights of individuals. Legitimate Interests is therefore an appropriate lawful basis.

7. Approval and Review

Approved by: Data Protection Manager at the latest Data Audit
Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity.

LIA-03 – CCTV MONITORING

NOT USED

LIA-04 – DASHCAMS

1. Processing Description
Dashcams are used in vehicles for the purpose of recording road incidents.

2. Purpose Test

- to ensure accurate recording of incidents;
- to support insurance and legal processes;

- to promote safety and accountability.

3. Necessity Test

- real-time visual recording cannot be achieved without camera technology;
- alternative methods would not provide reliable evidence.

4. Balancing Test

Nature of Data
Video footage in public spaces.

Reasonable Expectations
Individuals in public spaces have a reduced expectation of privacy.
Impact
Low, as:

- footage is not actively monitored;
- retention is limited;
- access is restricted.

Risks to individuals
The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

- limited retention;
- secure storage;
- controlled access.

5. Proportionality (DUAA)
Processing is limited to what is necessary and is proportionate to safety and evidential purposes.

6. Conclusion
The processing is justified under Legitimate Interests.

7. Approval and Review

Approved by: Data Protection Manager at the latest Data Audit
Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity

LIA-05 – USE OF ARTIFICIAL INTELLIGENCE (GENERATIVE AND AGENTIC)

1. Processing Description

The organisation uses approved Artificial Intelligence (AI) technologies, including Generative AI and Agentic AI, to support authorised business activities.

Generative AI is used to assist with research, drafting, summarisation, translation, analysis and document production.

Agentic AI may be used to automate approved business processes, monitor information sources, coordinate workflows and undertake authorised tasks under appropriate human oversight.

AI systems are used as business support tools and do not replace organisational accountability or human decision-making.

2. Purpose Test

The purposes of the processing are:

- to improve organisational efficiency and productivity;
- to support research and information analysis;
- to assist in the preparation and review of business documents;
- to improve consistency and quality of work;
- to automate appropriate low-risk administrative processes;
- to enhance service delivery while maintaining appropriate human oversight.

These purposes are legitimate organisational interests and support the efficient operation of the organisation.

3. Necessity Test

The use of AI is considered necessary because:

- AI enables routine tasks to be completed more efficiently and consistently;
- it assists staff in managing increasing volumes of information;
- automation reduces repetitive administrative activity while allowing staff to focus on higher-value work;
- appropriate human oversight is maintained over material decisions and outputs;
- no less intrusive and equally effective alternative would achieve the same operational benefits.

The organisation has determined that the processing is a proportionate and effective means of achieving these purposes.

4. Balancing Test

(a) Nature of the Data

The organisation seeks to minimise the use of personal data within AI systems.
Where personal data is processed, it is limited to that which is necessary for the authorised business purpose.

Special category data and criminal offence data must not be processed using AI unless specifically authorised, supported by an appropriate lawful basis and condition for processing, and subject to additional safeguards.

(b) Reasonable Expectations

Individuals would reasonably expect organisations to make use of modern technologies to improve efficiency and service delivery, provided that such technologies are used responsibly, transparently and in accordance with applicable data protection legislation.

(c) Impact on Individuals

The impact on individuals is limited because:

- AI is used to support, rather than replace, human judgement;
- outputs are reviewed by appropriately authorised personnel before reliance is placed upon them where necessary;
- AI is not used to make solely automated decisions producing legal or similarly significant effects unless separately authorised and compliant with applicable legislation;
- the organisation applies data minimisation principles when using AI.

(d) Safeguards Implemented

The organisation applies the following safeguards:

- use of approved AI systems only;
- compliance with the Artificial Intelligence Policy;
- data minimisation principles applied to all prompts and processing;
- prohibition on entering unnecessary personal data into AI systems;
- prohibition on using personal AI accounts for organisational information unless expressly authorised;
- appropriate access controls and authentication;
- human oversight of outputs and actions;
- audit logging where available;
- regular review of AI use and associated risks;
- staff training and awareness.

Where Agentic AI is deployed, additional controls include:

- defined authority limits;
- approval requirements for autonomous actions;
- monitoring of automated activities;
- the ability to suspend or terminate automated processes where necessary.

(e) Vulnerable Individuals / Safeguarding Context

Where AI processing may involve vulnerable individuals or safeguarding-related information, additional organisational safeguards shall be applied.

Such information should not be processed using AI unless specifically authorised and appropriate technical and organisational measures have been implemented.

5. Proportionality Assessment (DUAA-Aligned)

The organisation has assessed that:

- AI processing is limited to defined and legitimate organisational purposes;
- personal data is minimised wherever practicable;
- appropriate technical and organisational safeguards have been implemented;
- the benefits of improved efficiency, consistency and service delivery outweigh the limited impact on individuals;
- no less intrusive means would achieve the same operational outcomes.

The processing is therefore considered reasonable and proportionate in the circumstances.

6. Conclusion

The organisation has concluded that:

- the processing is necessary for legitimate organisational purposes;
- it does not override the rights and freedoms of individuals;
- appropriate safeguards are in place to ensure lawful, fair and transparent processing.

Accordingly, reliance on **Article 6(1)(f) UK GDPR – Legitimate Interests** is justified where this lawful basis applies.

Where another lawful basis under Article 6 UK GDPR is more appropriate for a particular processing activity, that lawful basis shall be relied upon instead.

7. Review and Monitoring

This assessment will be reviewed:

- annually;
- following any significant change to AI technologies or organisational use;
- following any relevant security incident, data breach or complaint;
- following significant legislative, regulatory or guidance changes relating to AI or data protection.

Approved by: Data Protection Manager at the latest Data Audit
Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity.