WorkInConfidence Terms of Use and Policies [GCloud 15]

Where applicable GCloud 15 Call off Contract applies in priority to these terms.

WorkInConfidence Limited ("WorkInConfidence", "we" or "us"), the owner and operator of WorkInConfidence (the "Service") is a company incorporated in England and Wales with registered address at 2 Hoathly Road, East Grinstead, RH19 1RB, United Kingdom, and registration number 08255296. Use of the Services and our website is subject to:

For Client Organisations:

- Organisation Master Agreement (which covers our relationship with client organisations) (v2.3.3 last updated 28th January 2026)
- Joint Controllers Agreement (V1.0.1) [Unless we otherwise agree we act as Joint Data Controller with our client organisations] Last updated 4th July 2025.
- Data Processing and Sharing Agreement (V2.3 last updated 9th February 2021.) [Relevant if we expressly agree that we are Data Processor rather than Joint Controller.

For Individuals Using WorkInConfidence or what3things:

- Individual Terms (which cover our relationship with individual users of our Service) (v2.3.2 last updated 28th January 2026).
- Privacy Policy & Cookie Policy (v2.4.4 last updated 28th January 2026)

Organisation Master Agreement for all WorkInConfidence services

Organisational Master Agreement ("Master Agreement") (V 2.3.3 last updated 28th January 2026)

This Master Agreement and the Order Form constitute a contract between WorkInConfidence Limited (a company registered in England and Wales with registered address at 2 Hoathly Road, East Grinstead, West Sussex, England, RH19 1RB and registered number 08255296), ("WorkInConfidence", "we" or "us"), and the client organisation identified in the Order Form ("Customer", "you" or "your").

This Master Agreement governs the relationship between us and the relevant client organisation. If you are an individual user, the Individual Terms of Use ("Terms of Use") apply to you.

If there is any conflict or inconsistency between any provision of this Master Agreement and an Order Form, then the provisions of the Order Form shall prevail.

Definitions

"Authorised User" shall mean any person you authorise to use the Service(s) expressly or impliedly.

"Customer Interface" means where we have indicated that the Service can be self-administered, the web-based interface by which Customer and Authorised Users may access the Service.

"Intellectual Property Rights" means patents, copyright, moral rights, trademarks and service marks, goodwill, trade secrets, design rights, rights in computer software, database rights, know-how and any other intellectual property rights, registered or unregistered, and all similar rights in any part of the world.

"Service" means the WorkInConfidence online staff engagement and communications platform including its features and functionalities and / or what3things.net if appropriate.

"Software" means the software application(s) used by WorkInConfidence to provide the Service and any enhancements thereto.

"Term" means the term of the Master Agreement set out in the Order Form or otherwise in writing (including email), including any period by which any originally agreed term is automatically extended.

"User Input" means input and content provided or uploaded by Authorised Users to the platform, including answers to questions, posts to discussion boards, or individual replies within an anonymous dialogue.

"User Subscriptions" means the user subscriptions purchased by the Customer pursuant to clause 8 (Fees) which entitle Authorised Users to access and use the Services in accordance with this Master Agreement.

2. User Subscriptions

2.1 Subject to the Customer purchasing the User Subscriptions in accordance with clause 3.3, the restrictions set out in this clause 2 and the other terms and conditions of this Master Agreement, WorkInConfidence hereby grants to the Customer a non-exclusive, non-transferable right, without the right to grant sublicences, to permit the Authorised Users to use the Services during the Term solely for the Customer's internal business operations.

2.2 In relation to the Authorised Users, the Customer undertakes that:

2.2.1 the maximum number of Authorised Users that it authorises to access and use the Services shall not exceed the number of User Subscriptions it has purchased from time to time;

2.2.2 it will not allow or suffer any User Subscription to be used by more than one individual Authorised User unless it has been reassigned in its entirety to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access or use the Services; and

2.2.3 each Authorised User shall keep a secure password for his use of the Services and that each Authorised User shall keep his password confidential.

2.3 The Customer shall not access, store, distribute or transmit any viruses, or any material during the course of its use of the Service that:

2.3.1 is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

2.3.2 facilitates illegal activity;

2.3.3 depicts sexually explicit images;

2.3.4 promotes unlawful violence;

2.3.5 is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

2.3.6 is otherwise illegal or causes damage or injury to any person or property;

and WorkInConfidence reserves the right, without liability or prejudice to its other rights to the Customer, to disable the Customer's access to any material that breaches the provisions of this clause.

2.4 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Service and, in the event of any such unauthorised access or use, promptly notify WorkInConfidence.

2.5 Where Customer grants access to the Service to any third party it shall be responsible for actions of such third party.

3. Additional User Subscriptions

3.1 Subject to clause 3.2 and clause 3.3, the Customer may, from time to time during any term, purchase additional User Subscriptions in excess of the number set out in the Order Form or otherwise agreed in writing (including email) by the parties and WorkInConfidence shall grant access to the Service to such additional Authorised Users in accordance with the provisions of this Master Agreement.

3.2 If the Customer wishes to purchase additional User Subscriptions, the Customer shall notify WorkInConfidence in writing (including email). WorkInConfidence shall evaluate such request for additional User Subscriptions and respond to the Customer with approval or rejection of the request.

3.3 If we approve your request to purchase additional User Subscriptions, you shall, within 30 days of the date of the our invoice, pay to us the relevant fees for such additional User Subscriptions and, if you purchase such additional User Subscriptions part way through the any Term, such fees shall be pro-rated from the date of activation for the remainder of the relevant Term.

4. The Service

4.1 WorkInConfidence will provide the Service to Customer and Authorised Users during the agreed Term. WorkInConfidence may delegate the performance of certain portions of the Service to third parties, provided WorkInConfidence remains responsible to Customer for the Service.

4.2 WorkInConfidence will host, or have hosted for it, and maintain the Customer Interface, and provide the Customer and Authorised Users access to the Customer Interface via password protected Authorised User accounts. WorkInConfidence may in its discretion modify the Service(s) without adversely affecting them.

4.3 For Customers in the UK, the Services will be hosted in the United Kingdom. For Customers in the EU, the Services will be hosted in the UK if permitted under EU law otherwise in the EU. For Customers outside the UK and the EU the Services will be hosted in the UK or other legally permissible jurisdiction.

4.4 You acknowledge that subject to its taking steps to comply with its legal obligations or orders of relevant law enforcement authorities, WorkInConfidence will take all reasonable and proper steps to ensure confidentiality of Authorised Users and User Input. In particular, WorkInConfidence will only disclose the identity of any Authorised User or User Input to a Customer or any other third party if such disclosure is part of the relevant Service or if the relevant Authorised User has given us their permission. Unless such disclosure is a part of a Service, we do not provide access to identities of Authorised Users to you, nor provide access to identities of Authorised Users or User Input to any government or law enforcement authority. When someone requests WorkInConfidence to disclose the identity an Authorised User or User Input, they must follow the applicable legal process and serve on us the relevant order or injunction. We will review all requests for disclosure to ensure they are valid and only provide details that are necessary to comply with the relevant order or injunction.

Unless ordered by a law enforcement authority, we will not disclose any identity of an Authorised User to any Customer to aid any disciplinary proceedings.

4.6 We will, as part of the Service and at no additional cost to you, provide you with the our standard customer support services during normal business hours (i.e. between 9 a.m. and 5 p.m. on business days). We may review the scope, extent and frequency of the support services we provide to you and inform you in writing (including email) if we propose any changes to structure of fees we charge to you.

5. Restrictions on Use of Service

5.1 Customer agrees not to:

a. use any automated system to access the Service or collect any personally identifiable information from the Service nor use the Service for any commercial solicitation purposes.

b. attempt to compromise the Service integrity.

c. take any action that imposes an unreasonable load on our system.

d. upload invalid data, viruses, or other malicious code.

e. impersonate another person or misrepresent your relationship with a person or entity.

f. interfere with working of the Service.

g. use any information about the Service with a view to copying the Service or developing a competing service.

h. attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the software used or made available in the provision of the Service, in any form or media or by any means; or;

i. license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Service available to any third party except the Authorised Users;

j. attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the software made available in the provision of the Service .

5.2 The Customer shall comply with, and use all reasonable endeavours to ensure all Authorised Users comply with, the Individual Terms of Use.

5.3 Customer agrees to take reasonable steps to ensure that Authorised Users do not post or submit User Input that: (i) may create a risk of harm, physical injury or emotional distress (ii) may constitute a crime or tort; (iii) contains content that is unlawful, abusive, racially or ethnically offensive, defamatory, harassing, libellous, threatening, or otherwise objectionable.

5.4 WorkInConfidence is not responsible for any public display or misuse of User Input, except in the case of gross negligence or intentional misconduct by WorkInConfidence. Unless agreed otherwise, we may use information we collect (including User Input) to provide aggregated analysis of types of dialogues within or across organisations, provided that it does not compromise the identity of any individual or organisation or use information which is or might reasonably be regarded as commercially sensitive.

5.5 If the Customer or any Authorised Users breach this Master Agreement or the Terms , we may suspend or terminate the provision of the Service (or their part) to the Customer or individual Authorised Users, provided that we act proportionately.

6. Access to the Service

6.1 Customer is responsible for providing, installing and maintaining at its own expense all equipment and facilities necessary to enable Authorised Users to use the Service.

6.2 Where Service requires it, WorkInConfidence will issue a user identification to each Authorised User to enable the Authorised User to access the Service. Customer will immediately notify WorkInConfidence of any breach of security known to it.

6.3 WorkInConfidence may on reasonable notice temporarily limit use of the Service(s) to make modifications, or do so without advance notice as a result of circumstances beyond WorkInConfidence's reasonable control.

7. Right to Monitor Use of the Service

WorkInConfidence has the right to monitor use of the Service to ensure compliance with this Master Agreement. WorkInConfidence will also have the right to analyse Authorised User behaviour to measure use of the Service on an individual and aggregate basis and otherwise to create metadata about use of the Service provided that such metadata is never disclosed to any third party other than in an anonymised and aggregated format.

8. Fees

8.1 Customer will pay WorkInConfidence the fees agreed by the Parties in an Order Form or otherwise in writing (including email). WorkInConfidence will invoice Customer, and Customer shall pay amounts due within thirty days of the date of invoice. Customer will pay any relevant taxes (such as sales taxes and VAT).

8.2 If the Customer signs up for the Service via online payment, Customer will be charged on the following basis:

a. the standard fee for the package you sign up for (less any agreed discounts). Any fees for packages paid in advance are not refundable.

b. if you sign up for an ongoing periodic package (monthly or yearly), we will be entitled to rebill you at the completion of any period for renewal for the next such period unless you notify us of your intention to terminate this agreement at least 30 days before the end of its Term or any subsequent renewal period.

c. if you upgrade your package within a billing period you will be charged the pro rata increase for the remainder of your billing period immediately, and at the new package rate on the commencement of the next billing period.

d. We do not give refunds on a downgrade but if you downgrade during a billing period your current package will remain available for the remainder of the billing period. At the end of the billing period you will be charged at the new package rate.

e. if you have given credit card details and are on a periodic plan we are authorised to use them to bill you upon a renewal unless you have notified us of your intention to terminate this agreement at least 30 days before the end of its Term or any subsequent renewal period. If we don't have a credit card on file, or it is declined or has expired, unless you have cancelled prior to the start of a billing period you will be liable to us for the relevant fees.

f. We may use a third party payment provider to facilitate payment to us.

g. We reserve the right to change our monthly fees upon a minimum of 30 days' notice. For clients who have paid in advance any price increase would only be implemented on next renewal.

9. Ownership

9.1 Customer shall retain all ownership rights to the User Input and may view and access User Input on a selective basis using the functionality of the Service. User Input cannot be bulk extracted from the relevant Service unless WorkInConfidence has agreed to make this facility available to the Customer. Post termination of this Master Agreement, WorkInConfidence shall within a reasonable time frame delete such information from the relevant Service, without need to consult Customer, unless a run off period for continued access to the Service has been agreed with the Customer. Customer agrees that WorkInConfidence acts as a conduit for the exchange and publication of the User Input. WorkInConfidence will not review or distribute any User Input except as provided herein, or as is apparent from the Service or as required by law.

9.2 If the Customer and/or Authorised Users submit comments or ideas about the Service to WorkInConfidence, the Customer agrees that WorkInConfidence may use them on a non-confidential basis unless they are clearly confidential.

10. Term

10.1 This Master Agreement will commence as agreed between the parties in writing, or when the Customer accepts these Terms by starting to use the Service and, unless otherwise agreed, will end when terminated by one month's notice from either party to the other, not to expire before the completion of any fixed term.

10.2 If the parties have agreed in any proposal and acceptance of that proposal for a multi-year contract the term and pricing in such proposal shall apply. If an automatic renewal has been agreed unless notice has been given such automatic renewal shall apply for any agreed period unless such notice has been given. On any multi-year contract pricing agreed at the outset shall apply for such multi-year period, otherwise on any renewal WorkInConfidence shall be entitled to increase pricing by the higher of 3% and RPI in the last year.

10.3 Either party may terminate this Master Agreement if:

a. the other commits a material irremediable breach, or where such breach is remediable, fails to remedy such breach within 30 days of notice;

b. the other party takes any step or action in connection with its entering administration, provisional liquidation or any composition or arrangement with its creditors (other than in relation to a solvent restructuring), being wound up (whether voluntarily or by order of the court, unless for the purpose of a solvent restructuring), having a receiver appointed to any of its assets or ceasing to carry on business or, if the step or action is taken in another jurisdiction, in connection with any analogous procedure in the relevant jurisdiction:

the other party suspends, or threatens to suspend, or ceases or threatens to cease to carry on all or a substantial part of its business; or

the other party's financial position deteriorates to such an extent that in the terminating party's reasonable opinion the other party's capability to adequately fulfil its obligations under the Master Agreement has been placed in jeopardy.

10.4 Upon termination (a) any right to use the Service will cease; (b) each party will if requested destroy all confidential information of the other; (c) WorkInConfidence will have no further obligation to provide the Service; (d) Customer will pay WorkInConfidence any amounts due.

11. Limitation of Liability

11.1 To the extent permitted by law:

a. WorkInConfidence assumes no responsibility for any (i) errors of content; (ii) interruption or cessation of the Service; (iii) User Input and its reliability, integrity, accuracy and quality; or (iv) the defamatory, offensive, or illegal conduct of any third party.

b. WorkInConfidence, its affiliates, directors, officers, employees or agents shall not be liable for any indirect, special, consequential or exemplary loss or damages, including without limitation damages for loss of income, loss of profits or goodwill arising out of or in connection with use of the Service, or otherwise.

c. WorkInConfidence, its directors, employees, or agents shall not be liable for any amount exceeding the amount the Customer paid to WorkInConfidence in the 12 months prior to the action giving rise to the liability.

11.2 Nothing in this Master Agreement shall limit or exclude our liability for death or personal injury caused by our negligence, for fraud or fraudulent misrepresentation or for any other liability which cannot be properly excluded under English law.

12. Third Party Claims

12.1 If the Software and/or the Service become, or, in WorkInConfidence's reasonable opinion are likely to become, the subject of a third party infringement claim, WorkInConfidence shall have the right to (i) replace or modify the Service so that they become non-infringing, or (ii) terminate the Service and provide a prorated refund of fees.

12.2 WorkInConfidence will have no liability for any claim to the extent it is based on improper use of the Software or Service; use of the Software or the Service in combination with any other software.

13. Confidentiality

13.1 Each party will use reasonable steps to keep confidential information of the other confidential. For the purposes of this clause "Confidential Information" means information designated as confidential or which would reasonably be considered to be confidential.

13.2 The parties shall not publish or disclose to any third party any Confidential Information, nor use the Confidential Information for any purpose other than to perform its obligations under this Master Agreement.

13.3 The confidentiality obligations above do not apply to information which:

(a) is already in the public domain;

(b) is published or comes into the public domain by means other than an action or omission on the part of the relevant party;

(c) a party can demonstrate was known to them or subsequently independently developed by them not using or derived in any way from the Confidential Information;

(d) is required to be disclosed by applicable law or court order or regulatory body (the party so required shall promptly notify the other of such request);

13.4 The foregoing confidentiality obligation shall apply during the term and for five years after the expiration of this Master Agreement.

14. Service Levels

14.1 We aim that the Service is available at least 99% of the time, apart from reasonable scheduled maintenance (either outside normal business hours or up to 1 day per quarter). If do not meet this target, your sole and exclusive remedy will be for us to provide the Service to you for additional 7 days after the expiration of the term of the Master Agreement free of charge, provided you request this within 28 days of the relevant outage.

14.2 WorkInConfidence does not warrant that:

(i) the Customer's use of the Service will be uninterrupted or error-free;

(ii) the Service or the information obtained by the Customer through the Service will meet the individual requirements of the Customer; or

(iii) the Service will be free from vulnerabilities or viruses.

14.3 WorkInConfidence is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Service may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

15. Miscellaneous

15.1 This Master Agreement, and any rights granted hereunder, may not be transferred or assigned by you. We may assign it provided that suitable arrangements are put in place to ensure ongoing delivery of our obligations.

15.2 Notices hereunder shall be in writing (including email) and sent to the registered office of the relevant party, or other notified address. Notice shall be deemed received two days after the date of posting.

15.3 This Master Agreement is governed by English law and subject to the exclusive jurisdiction of the English Courts.

15.4 This Master Agreement, together with any other legal notices and agreements published by WorkInConfidence, shall constitute the entire agreement between the Customer and WorkInConfidence.

15.5 Any waiver by either party of a provision hereof shall not be construed as a waiver of any other provision. If any provision of this Master Agreement is deemed invalid by a competent court it shall not affect the validity of the remaining provisions.

15.6 WorkInConfidence may provide notifications, whether such notifications are required by law or are for marketing or other business related purposes, to you via email notice, written or hard copy notice, or through posting on our website.

15.7 If WorkInConfidence have to change this Master Agreement we will notify you by email to the email address you gave to us when you registered with us.

15.8 No agency, partnership or joint venture relationship is intended or created by this Master Agreement.

15.9 Please contact help@WorkInConfidence.com with any questions regarding this Master Agreement.

Joint Controllers Agreement (v. 1.0.1)

The Agreement between:

This Joint Controller Agreement along with Master Agreement and the Order Form constitute a contract between WorkInConfidence Limited (a company registered in England and Wales with registered address at 2 Hoathly Road, East Grinstead, West Sussex, England, RH19 1RB and registered number 08255296), ("WorkInConfidence", "WIC", "we" or "us"), and the client organisation identified in the Order Form ("Customer").

1. Background

a) Customer and WIC agree to work together to allow Customer's employees to access the WorkInConfidence.com platform for the purpose of giving employees an independent platform to voice workplace concerns and provide feedback and views.

b) WIC works to ensure the identity of individuals who voluntarily choose to register on the platform are not disclosed to the Client, where this represents the wishes of individuals unless said individuals choose to self-identify.

c) The Customer uses the platform for the purposes of sharing Personal Data (to provide access to the platform and enable use of it) of eligible registrants, as well as managing messages received, Consolidated Case Management (CCM), discussion boards and surveys.

d) This Agreement sets out the responsibilities of each of the parties above in areas relating to the protection, security, sharing and processing of Personal Data that one or more of the parties require in order to conduct their individual or shared objectives and activities.

e) This Agreement is intended to document compliance with the UK GDPR and the UK Data Protection Act 2018 (Data Protection Legislation) and EU Data Protection legislation.

f) In this document, (i) headings are included for convenience only and shall not affect the construction or interpretation of this document; (ii) any reference to a paragraph shall (unless expressly provided otherwise) be a reference to a paragraph of this document; (iii) any reference to the singular shall include the plural and vice versa and any reference to one gender shall include all genders including the neuter gender, (iv) any reference to a person shall, unless the context otherwise requires, include individuals, partnerships, companies and all other legal persons; (v) the words "include", "includes", "including" and "included" will be construed without limitation unless inconsistent with the context; and (vi) any reference in this document to law or to any statute, statutory instrument, directive, regulation, order or other enactment shall mean the same as shall be amended, enacted, replaced, extended, modified, consolidated or repeated from time to time.

2. Interpretation

The following definitions apply in this Agreement:

Controller, Controllers, Processor, Data Subject and Personal Data, Special Category Personal Data, processing/processed and Appropriate Technical and Organisational Measures shall have the meanings given to them in the applicable Data Protection Legislation.

Data Protection Authority: a national authority, as defined in the Data Protection Legislation: for the UK, this is the Information Commissioner's Office.

Data Protection Legislation: The UK Data Protection Act 2018 and UK GDPR (the Retained Regulation (EU) 2016/679, as retained in UK law by means of the EU Exit Regulations 2019 (SI 2019/419)), any EU law or regulation applicable to Customers in the EU.

Individual Privacy Rights: refers to individuals' rights as set out in Articles 12-23 of UK GDPR or equivalent EU law.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Related Personal Data.

Purpose/Purposes: has the meaning given to it in clause 3 of this Agreement.

Related Personal Data: the Personal Data shared and/or processed between the parties for the stated Purpose.

Registered Users/Registrants: Data Subjects who have been provided with voluntary access to the Platform by the Customer.

3. Purpose

a) The purpose of the agreement is to agree the respective rights and obligations of the Parties in relation to GDPR and for the Customer to grant WIC with the licence to provide the WorkInConfidence platform.

b) In providing this service WIC will act as the Controller of Related Personal Data for the following purposes:

i. Registration process;

ii. Implementing measures to protect the identity of registrants from being disclosed to the Customer (unless the registrant actively chooses to disclose their identity to the Customer via the platform);

iii. Ensuring the implementation of robust security measures within the platform; and

iv. Ensuring any third-party suppliers contracted to provide the service meet their data protection obligations.

c) In using this service the Customer will act as a Controller of any Personal Data processed for the following purposes:

i. Providing email addresses to WIC for the purpose of registration;

ii. Assigning manager or admin status to individuals within the Customer's organisation;

iii. Managing Consolidated Case Management (CCM);

iv. Managing Surveys; and

v. Managing Discussion Boards

4. Term of this Agreement

This Agreement shall apply from the date Customer first becomes a client of WIC and starts to use the WIC platform until the date all Customer data is removed from the WIC platform following Customer ceasing to be a client of WIC.

5. Compliance with Data Protection Legislation

a) In relation to the provision of the WorkInConfidence platform by WIC to the Customer, each party is responsible for and agrees to ensure it does all it is required to i in order to comply with applicable Data Protection Legislation at all times.

b) Both parties will collaborate, as necessary, in order to:

i. Comply with an Individual Privacy Rights requests at set out in Articles 15-22 of EU/UK GDPR;

ii. Respond to notices served upon them by a Data Protection Authority (e.g. The UK's Information Commissioner's Office);

iii. Respond to complaints from Data Subjects; and

iv. Investigate any breach or alleged breach of Data Protection Legislation.

c) Both parties will be responsible for ensuring the processing of Related Personal Data is conducted in line with the core data protection principles under UK GDPR.

d) WIC will retain Related Personal Data for the term of its licence, including agreed run off period.

e) At the termination of the llicence, WIC will delete Related Personal Data and if required provide a data destruction notification to the Customer.

6. Shared Personal Data

a) The following types of Personal Data may be shared between the parties via the platform:

i. Email addresses of individuals invited to register on the platform;

ii. Full name, job title and opinions expressed by individuals, but only in such circumstances where individuals chooses to disclose this to the Customer within the platform; and

iii. Any Personal Data actively requested or elicited by the Customer via the platform (for example via a survey).

7. Individual privacy rights procedure

a) The Parties agree to provide reasonable assistance to each other, where necessary, to facilitate the handling of any Individual Privacy Rights requests.

b) For the avoidance of doubt, where such a request is received by WIC, and relates to Data Subject who has not disclosed their identity to the Customer, WIC will take sole responsibility for fulfilling the request.

8. Security incidents and reporting procedures

a) The Parties agree to provide reasonable assistance to each other to facilitate the handling of any data security incident in an expeditious and compliant manner.

b) The Parties should notify each other without any undue delay of any relevant potential or actual losses of Related Personal Data and remedial steps taken, either through mechanisms specified by the parties from time to time or otherwise to the named contacts in this Agreement, to enable the parties to consider what further action is required either individually or jointly.

9. Data Security

a) WIC will ensure Appropriate Technical and Organisational Measures are implemented to protect Personal Data on its platform.

b) In circumstances where Personal Data is extracted from the platform the Customer is responsible for ensuring Appropriate Technical and Organisational Measures are implemented to protect Personal Data on its own internal systems.

10. Use, Disclosure and Publication

a) WIC commits to process Related Personal Data solely for the Purpose.

b) Related Personal Data shall not at any time be copied, broadcast, or disseminated to any other third Parties, except in accordance with this Agreement, or a party to it.

c) The only exceptions to clauses 10(a) and 10(b) are where disclosure is required by law and in the fulfilment of individual privacy rights requests.

d) During the term of this Agreement, WIC will limit access to Personal Data to authorised employees or third party suppliers;

i. that require such access to fulfil the Purpose.

ii. that require access to enable the fulfilment of individual rights requests.

iii. who are aware of and trained in relation to the confidential nature of Personal Data, and in the use, care, protection and handling of Personal Data; and

iv. who have committed themselves to confidentiality or are under an appropriate statutory duty of confidentiality.

e) For UK/EU Customers, no Personal Data supplied by the Customer or provided by Registered Users on the platform will be transferred to a country outside the UK or the EU by WIC, during the term of this Agreement, without gaining the agreement of both Parties. Personal Data transfers outside the UK or EU are restricted and if conducted, WIC agrees to ensure appropriate safeguards are in place in line with Article 45-46 of UK GDPR or other appropriate EU law.

(f) Without limiting the need to ensure appropriate safeguards if WIC requests permission to transfer outside of the UK or EU under sub clause (e) above, permission shall not be unreasonably withheld or delayed. Failure to give a valid reason for withholding consent within 10 business days of being notified of any proposed change shall be deemed as consent. If WIC reasonably deems this to be a necessary change or necessary service provider to reasonably maintain its service and Customer objects, WIC shall be entitled to terminate the contract with and provision to Customer provided that (i) it makes a proportion refund for any remaining part of the Agreement, and (ii) ensures a prompt, safe and orderly destruction of Customer data.

11. Destruction of Personal Data

In line with Clause 5 e) upon termination or expiry of this Agreement WIC shall delete all Related Personal Data and if requested by Customer provide a notification of such deletion to the Customer within 21 business days.

12. Term and termination

This Agreement shall commence on the date on which Customer first become a client of WIC and will continue for as long as Customer is a customer of WIC plus any agreed run off period during which data is to be retained.

13. Other

The WorkInConfidence Organisational Master Agreement also covers the relationship between the Parties.

Appendix A

WIC instructs the following third party Processors to provide services in order to fulfil the Purposes of this Agreement:

- Amazon Web Services (AWS): Security, hosting, data storage and email delivery
- CloudFlare: Network optimisation.

Appendix B

- All aspects of data security are included in both employee and contractor contracts
- Data transferred between the client and server is encrypted using SSL
- All customers have their information and conversations held in separate databases
- All passwords are salted and hashed
- The system insists that users select strong passwords
- Databases are regularly backed up
- Systems are in place to prevent intrusion and logs are automatically scanned for anomalies.

Data Processing And Sharing Agreement

NOTE: WorkInConfidence's standard relationship with its clients is that of Joint Data Controller. Click on the hyperlink to see our Joint Controller Agreement.

This is important for Us and clients so we can guarantee we will not be required to disclose user IDs.

There may be circumstances in which we agree (subject to suitable protections for user identities) to be Processor. In those circumstances this Data Processing and Sharing Agreement shall apply.

Capitalised terms used in this Data Protection Schedule have the meanings given in the Terms and Conditions, unless otherwise defined herein.

1. Additional definitions

1.1 "Data Controller", "Controller", "Data Processor", "Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "processing" shall have the meaning given to those terms in the Data Protection Legislation (providing that "Data Controller" and "Data Processor" shall be deemed to mean, respectively, "Controller" and "Processor" as such terms are defined in the General Data Protection Regulation) and "process" and "processed" shall be construed accordingly.

1.2 "Standard Contractual Clauses" means the European Commission's Standard Contractual Clauses according to the EU Commission decision of 05 February 2010 (2010/87/EU) attached hereto as Annex 3.

1.3 "Data Protection Legislation" means the UK Data Protection Legislation and any other European Union legislation relating to Personal Data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

1.4 "UK Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

2. The parties agree that:

2.1 for the purposes of the Data Protection Legislation, the Customer is the Controller and Work in Confidence Limited (WIC) is the Processor, where Annex 1 sets out the scope, nature and purpose of processing by the Processor, the duration of the processing and the types of Personal Data and categories of Data Subject.

2.2 Where a party is processing Personal Data in their capacity as a separate and independent Controller, each party shall at all times comply with the Data Protection Legislation and shall not, by its act or omission, cause the other party to breach the Data Protection Legislation.

2.3 The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Processor and/or lawful collection of the Personal Data by the Processor on behalf of the Customer for the duration and purposes of this Agreement.

2.4 To the extent any processing of EU Data by the Processor takes place in any country outside the European Economic Area in a country that does not provide an adequate level of protection of personal data (as recognized by the European Commission), then the parties agree that the Standard Contractual Clauses set out in Annex 3 will apply in respect of that processing of EU Data, and the

Processor will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter' in the standard contractual clauses.

3. Data Processor terms

3.1 Without prejudice to the foregoing, to the extent that one party is deemed to act as a Data Processor for the other party (as the Data Controller) in respect of Personal Data, the Data Processor shall in respect of such Personal Data:

3.1.1 only process Personal Data on the documented instructions of the Data Controller for the purpose of performing its obligations under this Agreement or as may be agreed in writing between the parties (and on written instructions from the Data Controller to ensure compliance with the Data Protection Legislation and shall not process the Personal Data for its own purposes);

3.1.2 to the extent permitted by law, immediately notify the Data Controller in writing if it believes it has been provided with any instruction to process the Personal Data in breach of the Data Protection Legislation;

3.1.3 use reasonable endeavours to notify the other party if it is obliged to make a disclosure of the Personal Data collected under or in connection with the Agreement under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law.

3.1.4 take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data collected under or in connection with the Agreement and against accidental, unauthorised or unlawful processing of, loss or destruction of, alteration or damage to, disclosure of, or access to, Personal Data and that, having regard to the state of technical development and the cost of implementing any measures, such measures will ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, alteration, or damage to or disclosure of, or access to the Personal Data and the nature of the Personal Data to be protected, and shall regularly review and update the technical and organisational measures implemented to keep the Personal Data collected under or in connection with the Agreement secure and confidential in order to demonstrate that the processing of the Personal Data is performed in accordance with the Data Protection Legislation;

3.1.5 take reasonable steps to ensure the reliability of all personnel who have access to Personal Data and ensure that only personnel who require access to the Personal Data are given access (and only to the extent necessary) and that such personnel: (i) are informed of the confidential nature of the Personal Data; (ii) have received appropriate training on protecting Personal Data; and (iii) are bound by contractual or statutory confidentiality obligations in relation to the Personal Data, and ensure that any such access is revoked once no longer required;

3.1.6 promptly notify the Data Controller if it receives a request pertaining to the exercise of a Data Subject right pursuant to the Data Protection Legislation, including without limitation, subject access rights, rights to rectification, restriction of processing, data portability, the right to object to processing and automated decision-making. The Data Processor shall not respond to a Data Subject request without the Data Controller's prior written instruction.

3.1.7 without undue delay upon discovery, notify the Data Controller of any actual or suspected Breach of this Schedule including a Breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed ("Personal Data Breach").

3.1.8 immediately provide such cooperation, assistance and information to the Data Controller, at the Data Controller's reasonable costs, as may be required to allow the Data Controller to comply with: (a) the completion of any data protection impact assessment as reasonably required from time to time pursuant to the Data Protection Legislation; (b) the data protection by design and data protection by default principles under the Data Protection Legislation; (c) the rights of Data Subjects pursuant to the Data Protection Legislation, including without limitation, subject access rights, rights to rectification, restriction of processing, data portability, the right to object to processing and automated decision-making; (d) notices served by any supervisory authority for data protection purposes, such as the Information Commissioner's Office in the UK; and (e) any other notification and the Data Controller's or the Controller's (as applicable) other obligations set out in the Data Protection Legislation;

3.1.9 at the Data Controller's reasonable costs, allow representatives of the Data Controller to audit its compliance with the requirements of this Schedule on reasonable notice, and/or on request, to provide evidence of its compliance with such requirements;

3.1.10 transfer Personal Data from the European Economic Area (EEA) to outside the EEA, the European Union (EU) or the UK (to the extent that the UK is no longer in the EEA or the EU) only on the basis that the Data Processor shall, and where applicable shall procure that its subcontractor shall, prior to any such transfer: (i) ensure there are in place appropriate safeguards to protect the Personal Data including (without limitation), ensuring there is in place with the Data Controller such further documentation as may be necessary for the transfers to be lawful; (ii) ensure there are in place enforceable Data Subject rights and effective legal remedies for Data Subjects as required by the Data Protection Legislation; and (iii) comply with any reasonable written instructions relating to the same from Data Controller from time to time

3.1.11 for users in the EU, not engage a sub-processor without prior specific or general authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the relevant Data Controller the opportunity to object to such changes. If no objection is received within 10 working days of the Data Controller being notified of any potential change then the sub processor is considered authorised. If the Data Controller rejects any reasonable change proposed by WIC, then WIC shall be entitled to terminate this Agreement and provision of its' services. Existing sub-processors are deemed to be authorized and listed in Annex 2. The Data Controller shall use only sub-processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the Data Subjects. Processing by a Data Processor shall be governed by a contract or other legal instrument governed by English law or the law of an EU Member State, that is binding on the Data Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller and shall contain terms not less protective that those in this Agreement, and

3.1.12 not later than 180 after the end of the Agreement, or if instructed earlier upon the request of the Controller as soon as reasonably practicable, permanently delete from its information technology systems all copies of Personal Data in its possession.

ANNEX 1: DETAILS OF DATA PROCESSING

(a) Subject matter: The subject matter of the data processing under this Data Protection Agreement is the provision of an online system (pc, mobile and tablet) to engage and understand staff better to deliver healthier organisations

(b) Duration of processing: WIC will process data only for the duration of the Agreement, unless instructed otherwise by UK law or otherwise agreed in writing.

(c) Nature and Purpose of processing: Onboarding of employees, hosting surveys, responses, feedback responses; management reporting

(d) Categories of data being processed:

(i) Emails, user names and passwords, job roles, mobile phone numbers

(ii) User created content (feedback, conversations, survey responses)

(e) Categories of data subjects:

(i) Employees and representatives of the Data Controller

(ii) Other stakeholders, persons or entities the Data Controller may choose from time to time to seek feedback, views or input from using the WIC platform.

ANNEX 2: LIST OF CURRENT SUB-PROCESSORS

Amazon Web Services (AWS): Security, hosting, data storage and email delivery

CloudFlare

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection both parties have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the WorkInConfidence client (controller) who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and

the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law

(and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) To send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9: Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established namely

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer warrants that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

A signed copy is available for the Data Exporter on request to WorkInConfidence.

Appendix 1 to the Standard Contractual Clauses

The Member States of any Data Controller may specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter: The relevant client of WorkInConfidence Limited.

The data exporter is (please specify briefly your activities relevant to the transfer):

See Annex 1 of the Data Processing Agreement

Data importer: The data importer is See Annex 1 of the Data Processing Agreement

Data subjects

The personal data transferred concern the following categories of data subjects: See Annex 1 of the Data Processing Agreement

Categories of data

The personal data transferred concern the following categories of data (please specify): See Annex 1 of the Data Processing Agreement

Special categories of data (if appropriate)

Special category data is not expected to be uploaded to the system but may be contained in feedback response, communications etc.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

See Annex 1 of the Data Processing Agreement A signed copy is available for the Data Exporter on request to WorkInConfidence.

DATA EXPORTER: WorkInConfidence Client

DATA IMPORTER: Name: WorkInConfidence Limited

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and where possible should be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c).

All aspects of data security are included in both employee and contractor contracts

Data transferred between the client and server is encrypted using SSL

All companies have their information and conversations held in separate databases

All passwords are salted and hashed

The system insists that users select strong passwords

Databases are regularly backed up

Systems are in place to prevent intrusion and logs are automatically scanned for anomalies.

Individual Terms of Use ("Terms") (v 2.3.2 last updated 28th January 2026)

1. Introduction

WorkInConfidence Limited is a company incorporated in England with registered office at 2 Hoathly Road, East Grinstead, West Sussex, England, RH19 1RB and registration number 08255296 ("WorkInConfidence", "we" or "us").

WorkInConfidence owns and operates Workinconfidence, an online staff engagement and communications platform and what3things.net. (the "Service") These terms apply to users of both.

These Terms are the terms on which we provide the Service(s) to you ("User(s)", "you" or "your"). By using the Service you accept these Terms.ur contract with an entity ordering and paying for the Service (our "Client Organisation") is set out in a separate Organisational Master Agreement ("Master Agreement"). Nothing in the Master Agreement limits your rights under these Terms of Use.

2. General Terms of Use

2.1 WorkInConfidence grants you a non-exclusive, non-transferable, non-assignable, revocable, right to use the relevant Service for so long as your Client Organisation has purchased a subscription for you.

2.2 The Services enable you to submit certain input and content to the platform, including answers to survey questions, posts to to discussion boards, or individual replies within an anonymous dialogue ("User Input"). You can also view responses and content submitted by other users.

2.3 WHERE WE SAY WE WILL HOLD OR PROTECT YOUR USER INPUT IN A CERTAIN WAY (SUCH AS PROTECTING YOUR IDENTITY) WE WILL TAKE ALL REASONABLE STEPS TO DO SO. We will only disclose your identity or User Input to a third party (including your employer or a law enforcement authority) if such disclosure is part of the relevant Service or if you have given us your permission. Unless such disclosure is a part of a Service, we do not provide access to user identities to employers, nor do we provide access to user identities or User Input to any government or law enforcement authority. When someone requests us to disclose your identity or User Input, they must follow the applicable legal process and serve on us the relevant order or injunction. We will review all requests for disclosure to ensure they are valid and only provide details of your identity or User Input that is necessary to comply with the relevant order or injunction. Unless ordered by a law enforcement authority or court or tribunal, we will not disclose your identity to your employer to aid any disciplinary proceedings.

2.4 Your User Input is owned by your Client Organisation, subject to our obligation to protect your indentity and anonymity. If you cease to be connected to your Client Organisation your access to Service will be terminated, but User Input submitted may remain available on the Service. If we have said your identify will be protected we will continue to protect it.

2.5 We do not monitor or verify User Input and take no responsibility for content you or anyone else uploads to the Services. The views expressed by other users of our Service do not represent our views or values.

2.6 We have put in places processes for suspending use for anyone who misuses the Service. If you come across anything in the Service that you consider to be defamatory, offensive or otherwise in breach of these Terms of Use, please contact us at help@workinconfidence.com so that we can look into it and, if appropriate, remove it.

2.7 We may change, update, or remove content from the Services at any time, at our sole discretion.

2.8 You may request at any time to delete information we hold about you from the Service, and we will do so in a timely manner. We are not obliged to remove any anonymised User Input (i.e. data that cannot be related to you or any other specific individual) which we process in providing the Service. In collecting information the confidential nature of our Servicemeans User Input is often not attached to the details of the person who input it – and this therefore cannot be removed from the Service in response to a request to do so.

3. Use of the Service

3.1 You are permitted to use the Services in accordance with their intended use and the relevant guidelines.

3.2 You agree to:

a) provide accurate and up-to-date information when using Service(s) (whilst it is not necessary, you may register with an alias email if you consider that is appropriate to protect your identity); and
b) keep your log-in details secure and confidential and promptly notify Us of any account security breach.

3.2 In using our Services, you agree to not to:

a) attempt to compromise the integrity of the Services;
b) use any automated system, such as a robot, to access the Service;
c) use the Service for non-intended commercial purposes such as marketing or promotional activities;
d) solicit log-in information, impersonate another person or access another person's account without permission;
e) submit User Input that might be considered malicious, discriminatory, bullying, harassing, offensive, inappropriate, defamatory or otherwise unlawful;
f) endeavour to upload any commercial communications, viruses or other malicious code.g. take action that imposes an unreasonable load on the Service(s).
g) breach or infringe any applicable laws, regulations, policies, or these Terms, or infringe any third party rights, or act in a way that is unlawful or fraudulent or has any unlawful purpose or effect.

4. Intellectual Property Rights

4.1 Except for User Input, all Intellectual Property Rights in relation to the Service are the property of, or have been licensed to, WorkInConfidence. Nothing herein shall create a license to any Intellectual Property Rights, and you agree not to license, modify, distribute or create derivative works from any such content.

4.2 For the purposes of these Terms, “Intellectual Property Rights” means patents, copyright, moral rights, trademarks and service marks, goodwill, trade secrets, design rights, rights in computer software, database rights, know-how and any other intellectual property rights, registered or unregistered, and all similar rights in any part of the world.

4.3 If you submit comments or ideas to us about the Service(s), unless you make it clear they are confidential, or that is apparent from their nature, you acknowledge and agree that we may use them as we wish and you hereby grant us a non-exclusive and transferable licence to do so for an unlimited term and territory.

5. Eligibility

Unless agreed otherwise with a Client Organisation, the Service is solely for use by persons aged 16 or older.

6. Cancellation or Suspension of Service

6.1 We may terminate or suspend your use of the Service if you:

a) breach these Terms.
b) cease to be connected to your Client Organisation or they ask us to remove or restrict your access.

6.2 We exclude our liability for all action we may take in response to breaches of these Terms. The actions we may take are not limited to those described above, and we may take any other action we reasonably deem appropriate.

7. Warranty and Limitation of Liability

7.1 The Services are provided on an “as is” basis, and use is at your own risk. The Service is provided without warranties, express or implied, insofar as permitted by law. Without limiting the foregoing, WorkInConfidence does not warrant that the Service will be available at any particular time or location.

7.2 Where our platform or Services contains links to other sites and resources provided by third parties, these links are provided for your information only. Such links should not be interpreted as approval by us of those linked websites or information you may obtain from them. We have no control over the contents of those sites or resources.

7.3 Subject to clause 7.4:

7.3.1 to the extent permitted by law, WorkInConfidence assumes no liability for (i) errors or inaccuracies of content; (ii) interruption or cessation of any Service; (iii) User Input submitted by any user, or any defamatory, offensive, or illegal conduct of any third party;

7.3.2 to the extent permitted by law, WorkInConfidence, its affiliates, directors, officers, agents, employees and licensors shall not be liable for any direct, indirect, special, consequential or exemplary loss or damages, including without limitation damages for loss of income, loss of profits or goodwill, whether in any action of contract, delict (including negligence), arising out of or in connection with your use of our websites or Services, or otherwise; and

7.3.3 in no event shall WorkInConfidence (or its affiliates, directors, officers, agents, employees or licensors) be liable for any amount exceeding the amount paid by your Client Organisation to Us in the 12 months prior to the action giving rise to the liability.

7.4 Nothing in these Terms shall limit or exclude our liability for death or personal injury caused by our negligence, for fraud or fraudulent misrepresentation or for any other liability which cannot be properly excluded under English law.

8. Security

8.1 We do not guarantee that our Service will be secure or free from bugs or viruses.

8.2 You are responsible for configuring your information technology, computer programmes and platform to access our Service. You should use your own virus protection software or ensure that your employer provides an appropriate virus protection software.

8.3 You must not misuse our Service by knowingly introducing viruses, trojans, worms, logic bombs or other material that is malicious or technologically harmful. You must not attempt to gain unauthorised access to our Service, the server on which our Service run or any server, computer or database connected to our platform or Service. You must not attack our platform or Service via a denial-of-service attack or a distributed denial-of service attack. We will report any such breach to the relevant law enforcement authorities and we will co-operate with those authorities by disclosing your identity to them. In the event of such a breach, your right to use our Service will cease immediately.

9. Assignment

9.1 These Terms, and any rights granted hereunder, may not be transferred or assigned by you.

9.2 WorkInConfidence may assign this agreement in whole or part provided that suitable arrangements are put in place to ensure proper ongoing delivery of our obligations.

10. General

10.1 These Terms are governed by English law and subject to the exclusive jurisdiction of the English Courts.

10.2 If any provision of these Terms is deemed invalid by a court it shall not affect the remaining provisions. No waiver of any term shall constitute a waiver of any other term.

10.3 Notices should be sent by registered post to WorkInConfidence's registered office address and will be deemed received two days later. We will send notices to you by email to the email address you are registered with and such notices shall be deemed given 24 hours later.

10.5 For questions about these Terms please contact help@workinconfidence.com.

Privacy Policy (v.2.4.4)

Who We Are

We are WorkInConfidence Limited, ("WIC") a company incorporated in England and Wales with registered address at 2 Hoathly Road, East Grinstead, West Sussex, England, RH19 1RB and registration number 08255296

We are registered with the ICO as a fee payer with registration number Z3403582

Our Data Protection Officer can be contacted by emailing dpo@workinconfidence.com

We provide a system which makes it easier for staff to give feedback to their organisation in a tried and trusted way.

1. Users of Our Platform and Our Role

This is the Privacy Policy for Users of the WorkInConfidence Online Platform / Web App including what3thing.net. Section 3 Below also applies to you.

We routinely act as a Joint Controller with your employer. Please note this is not always the arrangement. You can always contact your employer or WorkInConfidence (dpo@workinconfidence.com) if you would like further clarification.

Where we are Joint Controllers with your employer, we work together to allow access to the WIC platform for the purpose of giving employees an independent platform to voice workplace concerns and provide feedback and views IN A SAFE WAY WHERE YOUR IDENTITY IS PROTECTED (UNLESS YOU DECIDE AT ANY TIME TO SAY WHO YOU ARE).

WorkInConfidence specifically manages the registration process and the process of making sure the identity of people who voluntarily choose to register on the platform is not disclosed to their employer, where this represents the wishes of individuals. Unless people chose to self-identify, via the platform. Please also see our Individual Terms: https://www.workinconfidence.com/individual-terms/.

Your employer manages any personal data handled or collected for the following reasons; providing email address for registration purposes, assigning manager or admin status to specific employees, conducting surveys, running discussion boards, any case management conducted via the WIC platform, and any other circumstances in which you choose to self-identify. This does not affect our undertaking to protect your identity unless you decide or agree otherwise.

Where we are a Processor of personal data, we do so on the instruction of another organisation – probably your employer (the Controller). IF WE DO ACT AS PROCESSOR, WE STILL ENSURE THAT WE ARE IN A POSITION TO PROTECT YOUR IDENTITY (UNLESS YOU DECIDE AT ANY TIME TO SAY WHO YOU ARE).

For users or our platform we routinely process a work email address. For some people such as managers we may include name, job title, mobile phone number. You may also input certain other information and any personal details users provide via their use of the platform.

Your Rights

All individuals (users of our platform or otherwise) have a number of rights with regards to your personal data under the Data Protection Laws. If you wish to exercise any of your rights, please contact us at dpo@workinconfidence.com

- Right of access: You can request access to a copy of the personal data which we hold about you, as well as details about why and how we use it.;
- Right to rectification: You can ask us to change or complete any personal data we hold about you which is inaccurate or incomplete;
- Right to be forgotten/erasure: You have a right, under certain circumstances, to ask us to delete any personal data we hold about you. Please note that there may be situations where we must retain your personal data after a request for erasure where we have a lawful basis for doing so;
- Right of restriction: You can ask us to restrict (i.e. prevent) the processing of your personal data where you have objected to our use of it and we have no lawful basis to continue processing your personal data;
- Right of data portability: In certain circumstances, you can ask us to transfer the data we hold about you to another organisation. This would be sent in a structured, commonly used, electronic form;
- Right to object: You can object to us using your personal data for particular purposes; and
- Automated decision making: You have a right not to be subjected to automated decision making and profiling in certain situations.

If you have any cause to complain about our use of your personal data, please contact us by emailing dpo@workinconfidence.com

You also have the right to lodge a complaint about our processing with a supervisory authority — in the UK that is the ICO whose details are here: https://ico.org.uk/make-a-complaint/

Automated decision making

We do not use your personal data in any automated processes to make decisions about you

What Happens If Our Business Changes Hands?

We may, from time to time, expand or reduce our business and this may involve the sale and/or the transfer of control of all or part of Our business. Any personal data that you have provided will, where it is relevant to any part of our business that is being transferred, be transferred along with that part and the new owner or newly controlling party will, depending on the lawful basis, be permitted to use that data only for the same purposes for which it was originally collected by Us.

In the event that any of your data is to be transferred in such a manner, you will be contacted in advance and informed of the changes.

Changes to Our Privacy Policy

We may change this Privacy Policy from time to time (for example, if the law changes). We recommend that you check this page regularly to keep up-to-date.

If we make any material changes to the manner in which we process and use your personal data, we will contact you to let you know about the change.

Get in touch

If you have queries about our use of your data, please contact us by emailing us on dpo@workinconfidence.com

2. Other Individuals

In addition to the information provided above for users of our platform we also act as a Controller for the following type of individuals; WIC's employees, job applicants, suppliers, clients, prospects, investors and website visitors.

What Personal Data Does WIC Process?

You can find out more about the types of personal data we process for the above types of individuals here:

- I am a potential employee (see below section)
- I am a corporate client (see below section)
- I am a corporate prospect (see below section)
- I am a supplier to WIC (see below section)
- I am an investor/shareholder (see below section)
- I am just browsing your website (includes our cookie notice) (see below section)

Potential Employee Privacy Notice

Data that we hold and how we use it

As a potential employee we hold the following data on you:

Contact details, CV, and email correspondence with you. If you are successful in gaining employment with WIC then you will fall under the Employee Privacy Notice going forward.

Lawful basis for processing

Our lawful basis for processing your data is a combination of Contract, legitimate interest and consent. When you applied for a job it was with a view to entering into an employment contract with us. If we decide not to go forward with your application then we use legitimate interest to retain the data should the chosen candidate not work out or another role become immediately available.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our lawyers for contracting and to support with the visa sponsorship process if applicable. We do not sell your data to anybody.

Retention Periods

If you are unsuccessful in your application, we will keep your details on file for 3 months after the position is filled.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Corporate Client Privacy Notice

Data that we hold and how we use it

As a corporate client, we hold the contact details required to carry out our contract with you, data to manage our relationship and keep you up to date with changes and improvements to our services. This data would have been sourced from you directly.

Lawful basis for processing

Our lawful basis for processing your data is a combination of Contract and Legitimate Interest. We use legitimate interest when we use your data to keep you up to date with changes and improvements to our goods and services. Our legitimate interest balancing test indicates that this is a legitimate purpose; it is necessary for the purpose of keeping you updated and growing our business, and unlikely to cause you risk or harm. All other data is processed to enable us to fulfil our contract with you and manage our relationship with you.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our accountants to ensure we are paid appropriately. We do not sell your data to anybody

Retention Periods

We hold data on Corporate Clients for the length of time that you are a client of ours, then another 7 years in case of any dispute.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Supplier Privacy Notice

Data that we hold and how we use it

As a supplier to WIC, we hold the contact and payment details required to carry out our contract with you and data to manage our relationship with you. This data would have been sourced from you directly, although your contact details may have been sourced from a recommendation or another source, with the intention of entering into a contact with you.

Lawful basis for processing

Our lawful basis for processing your data is contract; all data is used enable us to fulfil our contract with you, including paying you and managing our relationship with you.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our accountants to ensure you are paid appropriately. We do not sell your data to anybody

Retention Periods

We hold data on suppliers for the duration of our contract, plus 7 years to account for accounting regulations and in case of any dispute.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Prospective Client Privacy Notice

Data that we hold and how we use it

As a potential client, we hold your name, job title and corporate contact details so we can build a relationship with you. This data will have been sourced directly from you at an event, or from your company website or a similar publicly available source. We only hold your data if we legitimately think you will have an interest in using our product.

Lawful basis for processing

Our lawful basis for processing your data is a Legitimate Interest for marketing purposes. As you are a corporate entity, we also abide by the Privacy and Electronic Communications Regulations (PECR). We give you the chance to opt out of all marketing on anything that we send you. We only share details of our own goods and services in our marketing. If your data was not sourced directly from you, then we contact you once we have the data to let you know that we have your data and give you the chance to opt out. Our legitimate interest balancing test indicates that this is a legitimate purpose: you would not be surprised to hear from us based on the nature of your job role, and our processing does not cause any harm or risk to you as a data subject.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We do not sell your data to anybody.

Retention Periods

We hold data on Potential Corporate Clients for 5 years, or until the point at which you opt out of communications. At this point you are added to a suppression list so we do not contact you again. When you become a Corporate Client, then that Privacy Notice for will apply.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes. All devices are protected by leading enterprise mobility management technologies. We are Cyber Essentials Plus certified.

Investor/Shareholder Privacy Notice

Data that we hold and how we use it

As an investor or private shareholder in WIC, we hold your contact and investment details. This data will have been sourced directly from you in the course of your investment.

We use this data to pass to the regulators, to issue your share certificates and to manage our relationship with you.

Lawful basis for processing

Our lawful basis for processing your data is a legal obligation, contractual obligation and legitimate interest. Our legitimate interest balancing test indicates that this is a legitimate purpose; you would not be surprised to hear from us based on the nature of our relationship, and our processing does not cause any harm or risk to you as a data subject.

Data Sharing and Transfers

We share your contact details in line with our regulatory requirements, so will be listed in official documents such as company filings and would be used in any potential data room.

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We do not sell your data to anybody.

Retention Periods

As a shareholder/investor we hold your information for as long as we are legally required to do so.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentification, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

3. Web Browsing Privacy Notice and Cookie Notice

Data that we hold and how we use it

As a web browser we collect information about you when you visit our website. This data includes information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our website that you visit, the time and date of your visit, the time spent on those pages and other usage statistics.

In addition, we use third party services such as Google Analytics that collect, monitor and analyse this data.

We use cookies solely to gather information on IP addresses, to analyse trends, administer the website, track your movements on our website and gather broad demographic information for aggregate use.

We are allowed to store cookies on your device if they are strictly necessary for the operation of Our sites. For all other types of cookies, We need your permission.

We ask you for consent to use cookies (where consent is required).

The cookies we use are as follows:

- On the WorkInConfidence web app / system we use only necessary cookies to enable you to have a good service:
- locale – stores the locale for the current user
- asideState – stores whether the function menu is open or closed
- trusted_device – stores whether you have enabled multi factor authentication
- PHPSESSID – the session details

On our marketing site we use cookies for the following::

- Leadworx to analyse use of our site
- Google Analytics to analyse use of our site
- A cookie to record whether you have accepted the cookie policy
- Bookify for arranging meetings.

Lawful basis for processing

For necessary cookies, we use legitimate interest as we need those cookies to exist for the website to work. For all other tracking we use consent. You can withdraw consent at any time by emailing dpo at workinconfidence.com

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example Standard Contractual Clauses.

Retention Periods

We hold data on our web visitors for up to 6 months.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes