Frontline Data Processing Agreement

This Data Processing Agreement (Agreement) is made between:

1 XXXXXXXX ('The Customer'), a company registered in England & Wales under registration number XXXXXXXX with a registered office of XXXXXXXXXXX

And

2 Uttlesford Citizens Advice Bureau ('The Provider'), a company limited by guarantee registered in England & Wales under registration number 3771142 and a charity registered under registration number 1078222 with a registered office of Barnards Yard, Saffron Walden, Essex, CB11 4EB

Whereas:

This agreement covers the use of: www.broxbournefrontline.org.uk, www.easthertsfrontline.org.uk, www.eppingforestfrontline.org.uk, www.harlowfrontline.org.uk, www.uttlesfordfrontline.org.uk and the 'Frontline Referrals' mobile application, all of which have been developed by or on behalf of the Provider.

(A) This Agreement is supplemental to Frontline user terms and conditions and any other separate agreement entered into between the parties and introduces further contractual provisions to ensure the protection and security of Personal Data processed by The Provider on behalf of The Customer.

(B) Data Protection Legislation (as defined below) imposes certain obligations upon a data controller to ensure that any data processor it contracts with provides sufficient guarantees to ensure that the processing of the Personal Data carried out on its behalf, is secure.

(C) This Agreement is entered into to ensure that there are sufficient security guarantees in place, and that the processing complies with obligations equivalent to those of the 7th Data Protection Principle and Article 28 of the General Data Protection Regulation.

It is hereby agreed as follows:

DEFINITIONS

Data Protection Legislation: (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

Personal Data and Data Subject: as defined in the Data Protection Legislation

1. Both parties will comply with all applicable requirements of the Data Protection Legislation. This Agreement is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

2. The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the data controller and the Provider is the data processor (where Data Controller and Data Processor have the meanings as defined in the Data Protection Legislation). [The Schedule sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject]

3. Without prejudice to the generality of clause 1, 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 Provider for the duration and purposes of this agreement.

4. Without prejudice to the generality of clause 1, the Provider shall, in relation to any Personal Data processed in connection with the performance by the Provider of its obligations under this agreement:

(a) process that Personal Data only on the written instructions of the Customer unless the Provider is required by the laws of any member of the European Union or by the laws of the European Union applicable to the Provider to process Personal Data (Applicable Laws). Where the Provider is relying on Applicable Laws as the basis for processing Personal Data, the Provider shall promptly notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Provider from so notifying the Customer;

(b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal

Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and

(d) not transfer any Personal Data outside of the UK;

(e) assist the Customer, at the Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Customer without undue delay on becoming aware of a Personal Data breach;

(g) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Applicable Laws to store the Personal Data; and

(h) maintain complete and accurate records and information to demonstrate its compliance with this Agreement [and allow for audits by the Customer or the Customer's designated auditor].

5. The Customer does not consent to the Provider appointing any third-party processor of Personal Data under this agreement.

6. Either party may, at any time on not less than 30 days' notice, revise this Agreement by replacing it with any applicable controller to processor standard clauses or similar terms forming party of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

Signed by [NAME OF APPROPRIATE PERSON(S)] for and on behalf of Customer

....
[Role]

Signed by [NAME OF APPROPRIATE PERSON(S)] for and on behalf of Provider

....
[Role]

THE SCHEDULE

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. PROCESSING BY THE PROVIDER

1.1 SCOPE

This agreement covers the use of: www.broxbournefrontline.org.uk, www.easthertsfrontline.org.uk, www.eppingforestfrontline.org.uk, www.harlowfrontline.org.uk, www.uttlesfordfrontline.org.uk and the 'Frontline Referrals' mobile application, all of which have been developed by or on behalf of the Provider.

The 'Customer' uses 'Frontline' to ensure that their clients are effectively signposted or securely referred to local social welfare services and/or that their service is able to receive signposts and/or secure referrals from other organisations.

The 'Customer' is expected to make/receive fewer than XXX referrals and signposts in a year.

1.2 NATURE

'Frontline' provides a 'Customer' with:

- a secure platform for social and welfare-based organisations to promote and maintain details about the services they offer
- a mechanism for organisations involved in health, education, social care, welfare and the public to search the site for service details, print or email service details or make a secure referral
- a mechanism for organisations to obtain statistics about their organisations signposting and referral activity.

'Frontline' will use data to:

- Securely transfer referral information from one 'Customer' to a different 'Customer' or a member of the public to a 'Customer'
- Monitor a referral to ensure that it has been actioned
- Distribute a periodic update on local services to registered users that have agreed to be on a mailing list
- Produce client anonymised statistics about referral and signposting activity between services
- Produce client anonymised statistics on the age and gender profile being referred through the system.

1.3 PURPOSE OF PROCESSING

To ensure that social welfare services can communicate and maintain details on their services in a format that is easily accessible to health, social care, education, council and community sector organisations.

To ensure that health, social care, education, council and community sector organisations can identify local social welfare services for their clients/ patients/ residents.

To ensure that registered users of ‘Frontline’ can send and receive referrals securely and that members of the public can self-refer securely.

To ensure that referrals made through the system are actioned.

To ensure that registered users who wish to get updates on service developments are provided with a periodic newsletter on developments.

To ensure that funders and ‘Customers’ of ‘Frontline’ have access to client anonymised activity statistics and client profile information to inform training and joint working initiatives.

1.4 DURATION OF THE PROCESSING

‘Frontline’ will continue to process data on behalf of the individual registered user under the ‘terms and conditions’ that are agreed and may be updated at any point in time.

Personal client data within an individual referral will be stored for a maximum of 90 days and will then be redacted indefinitely.

Inactive registered user information will be redacted after 1 year.

Client anonymised data will be stored for an indefinite period.

2. TYPES OF PERSONAL DATA

Client information:

Core mandatory fields for all referrals:

- First Name
- Last Name
- Date of Birth
- Address
- Postcode
- Phone number
- Reason for referral

Additional discretionary fields for all referrals:

- Email
- Additional telephone numbers
- Preferred method of contact
- Best time to call

An organisation creating an online referral form on ‘Frontline’ is also able to create additional mandatory or discretionary fields to ensure that they have the information they require to receive a good referral. This may potentially include a field that collects sensitive data if this is necessary (and authorised by a Frontline Administrator). Making a referral to an organisation, for example, a rape crisis service, a dementia support service or a LGBT support group may also indirectly communicate sensitive personal data.

Registered User information

- First Name
- Last Name
- Role
- Company Name
- Company Address
- Website
- Company/ Charity registration details
- Phone Number
- Email Address
- IP address

Customer information

- Number of registered users
- Activity of users (frequency and time using the sites)
- Number of referrals
- Number of signposts
- Referral activity by the Customer
- Referral activity to the Customer
- Signpost activity to the Customer
- Signpost activity from the Customer
- IP address if provided by the Administrator for easy log in

3. CATEGORIES OF DATA SUBJECT

Referred Client, Registered Users, Member of the Public

4. LAWFUL BASIS FOR PROCESSING THE DATA

Ensure that registered users can promote and maintain details of their services in a format that is easily accessible to health, social care, education, council and community sector organisations – Consent from registered user inputting and updating the data.

Ensure that one ‘Customer’ can securely send or receive a referral to/from another ‘Customer’ – Consent from client, recorded with an on-line tick box.

Ensure that a member of the public can make a secure self-referral to a ‘Customer’. Consent from client, recorded with an on-line tick box.

Monitor a referral to ensure that a referral has been actioned – Contract based on ‘Frontline’ Terms and Conditions.

Distribute a periodic update on local community services to registered users who have requested to be on a mailing list. Consent provided by registered users within their account.

Produce client anonymised statistics about referral and signposting activity between ‘Customer’ services. Legitimate interest

Produce client anonymised statistics on the age and gender profile being referred through the system. Legitimate interest.

Reviewed February 2021