Privacy Policy

As a data processor, ‘Frontline’ has always taken data security and management very seriously. ‘Frontline’ is a project developed and operated by and/ or on behalf of Uttlesford Citizens Advice Bureau of Barnards Yard, Saffron Walden, Essex, CB11 4EB. ‘Frontline’ refers to www.uttlesfordfrontline.org.uk, www.harlowfrontline.org.uk, www.eppingforestfrontline.org.uk, and the ‘Frontline Professional’ and ‘Frontline Public’ mobile applications.

‘Frontline’ helps community based health & wellbeing services promote themselves in one place and provides them a secure platform to receive and send on-line referrals and monitor signpost activities for their service. The public also have access to ‘Frontline’, to search for information about local services and make secure call back requests to participating services.

Please read the following carefully to understand how we treat your personal data. You should also read our terms and conditions of Registered Users, our public access terms and conditions, our policy on how we use Cookies and our disclaimer and copyright document. By visiting any ‘Frontline’ site you are accepting and consenting to the practices described in this policy and those documents.

Where we collect personal information from

Information you give us

For organisations with an account on ‘Frontline’ we collect information by you filling in forms on the websites or apps or by corresponding with us by phone, e-mail or otherwise. Information stored may include:

- details that are held in your account for example; your name; organisation details; website; email; phone numbers; names and emails of other people using your account; your agreement to send, receive or accept signposts; opening hours; information on how to access your service; data field requirements to accept a referral
- personal details of a client or patient that you are referring, together with the details of the service that you are referring to
- a recipient's email address and details of the service being signposted to.

We collect information from the public by you filling in a call back request, providing an email address to receive information about a service, providing on-line feedback on services and by corresponding with us by phone, email or otherwise.

Information we collect about you

With regard to each of your visits to 'Frontline' we may automatically collect the following information:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet; your login information; browser type and version; time zone setting; browser plug-in types and versions; operating system and platform
- information about your visit, including the full Uniform Resource Locators (URL); clickstream to, through and from our site (including date and time); page response times; download errors; length of visits to certain pages; page interaction information (such as scrolling, clicks, and mouse-overs); methods used to browse away from the page; and any phone number used to call our customer service number.

If you choose not to give personal information to us

You may choose to use 'Frontline' as an on-line resource for service information only, however we will continue to collect information automatically using Cookies if you accept them, for more information please read our 'How we use Cookies' policy.

Types of personal information collected and categories

We categorise the data we collect into three groups;

1) **Registered User information on Accounts in ‘Frontline’**

- First Name
- Last Name
- Company Name
- Company Address
- Website
- Company/ Charity registration details
- Phone Number
- Email Address
- IP address
- Security levels within ‘Frontline’
- Visits and time on ‘Frontline’
- Opt in to newsletter/service updates

2) **Account information**

- Number of Registered Users
- Referral activity by the service on each Account
- Referral activity to a service on each Account
- Signpost activity by the service on each Account
- Signpost activity to a service on each Account
- IP address if provided by the Administrator for easy log in
- Activity of users (frequency and time using the sites)

3) **Referred person information.** Personal data of someone being referred by a Registered User or member of the public

Mandatory fields:

- 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 an LGBT support group may also indirectly communicate sensitive personal data.

How we use your data

‘Frontline’ will use data to:

- ensure that Accounts can promote and maintain details of their services in a format that is easily accessible to all users
- ensure that all users can identify local health and wellbeing services
- ensure that all users can securely send referrals or self-refer to services that allow this facility
- monitor a referral to ensure that it has been actioned
- distribute a monthly update on local community services to Registered Users that have agreed to be on a mailing list
- contact all Registered Users when updating them on developments or changes in ‘Frontline’
- 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.

The legal basis of processing your data

We hold Account information and Registered User information on behalf of a Data Controller – the legal basis for holding this information is consent with the active agreement of clicking an on-line box of our ‘Registered User Terms and Conditions’. Data Controllers may also wish to supplement this legal basis with a formal processing agreement contract.

We securely transfer and monitor referrals and call back requests when a consent box has been ticked to ensure that consent has been given to share this information.

We distribute newsletters to Registered Users who record their agreement to receive this information within their Registered User account. This consent can be changed at any time by the user updating their account.

We will contact all Registered Users when updating them on important developments or changes in ‘Frontline’ on the basis of legitimate interest.

We will produce client anonymised statistics about referral and signposting activity between services and client anonymised statistics on the age and gender profile being referred through the system. Processing will be on the basis of legitimate interest.

Ownership of account information and data

Accounts on ‘Frontline’ are created and managed by organisations that use the system – as Data Controllers, they are responsible for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of the information stored and transmitted. We shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store data within your Account.

Although referral information has been shared with consent, data is still owned by the Data Controller providing the information.

If a member of the public uses Frontline, we will act as a Data Controller in this circumstance.

Client anonymised data and information about the use and activity of ‘Frontline’ by Accounts and the public is owned by ‘Frontline’.

Who we share your personal information with

Under the instruction of a Data Controller or consent of a member of the public we share personal referral information only with the service that has been selected to receive that referral.

We share client anonymised data and information about the use and activity of ‘Frontline’ by Accounts and the public with anyone who has a legitimate reason to review the data. This may include funders, health and wellbeing boards, Account holders and prospective organisations considering use of the platform.

How we keep your information safe

‘Frontline’ was designed as a secure, multi-agency referral system, here are some of the ways we ensure that your data is safe and that we are GDPR compliant:

- ‘Frontline‘ websites are hosted on the Microsoft Azure platform and data is stored within the EU
- Users of the system have individual passwords and enter the system using a secure login area, protected by an SSL certificate
- Organisations on the platform allocate individual users only the authorities required to access the data necessary for the role they undertake

- System training emphasises the importance of password security, confidentiality, client consent and only sharing information that is relevant to an effective referral
- A referral can only be made if a consent box is ticked
- Organisations on the platform can only see activity related to their own organisation
- Identifiable information about an individual is only held for a maximum of 90 days; after this time personal data is ‘blacked out’ and non-recoverable
- ‘Frontline’ apps communicate with the website using a secure REST based API, which is read-only for the library of services, and write only for submitting referrals so the app is not involved in any sensitive data transfer
- Everyone with access to the back office management system of ‘Frontline’ and are working or volunteering for/on behalf of the project are within organisations with embedded safeguarding policies and are suitably trained – provision of a copy of an annual Civil Service training certificate for General Security Awareness is mandatory
- Information held in individual Accounts can be edited and deleted on-line by Registered Users with administration rights at any time
- Personal information on a referral can be amended or corrected after transmission by a Registered User until the point that information is accessed by the service that is receiving the referral
- We keep encrypted disaster recovery files for a maximum of six months.

Although we make every effort to ensure the security and integrity of ‘Frontline’ and our associated communications and activities, unfortunately, no data transmission over the internet can be guaranteed to be 100% secure. As a result, while we use strict procedures and security features to try to prevent unauthorised access, ‘Frontline’ cannot ensure or guarantee the security of information when it is being transmitted.

Changes to our privacy policy

Any changes we make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our privacy policy.

Contact us about your information

If you have any questions about how your information is collected or used, you can contact us by:

Telephone - 01799 618855, open Monday to Friday 9.30am-3.30pm

Email - info@essexfrontline.org.uk

You can contact us to:

- find out what personal information we hold about you
- correct your information if it's wrong, out of date or incomplete
- request we delete your information
- ask us to limit what we do with your data - for example, ask us not to share it if you haven't asked us already
- ask us to give you a copy of the data we hold in a format you can use to transfer it to another service
- ask us to stop using your information

You can find out more about your data rights on the Information Commissioner's website.

Note: This privacy policy only covers the websites uttlesfordfrontline.org.uk, harlowfrontline.org.uk, eppingforestfrontline.org.uk and the 'Frontline' Mobile Applications. Other websites and services not managed by Frontline are not covered by this policy. Once you have accessed another site or service you will be subject to the security and privacy policy of that site or service.