

Privacy Policy



Privacy Policy

It is simple – information that is about you is private. Data Protection Legislation in the U.K. makes clear the responsibilities of data controllers and rights of data subjects such as you.

At ProblemShared, we respect and commit to protecting your personal data. Our Privacy Policy together with our Platform User Terms & Conditions explain the different types of data, how we collect, use, share, store your personal data and when we no longer hold your data, and what you can do about your personal data. This is in connection with when you interact with our Platform and any Service you receive over the Platform.

Our Policy is divided into different sections for ease of reference and you will find an index over page. Capitalised terms here have the same meaning as in the User Terms and Conditions, or in the Data Protection Legislation unless specified otherwise.



<u>Index</u>	<u>Page</u>
1. <u>About us and contact details</u>	<u>5</u>
2. <u>Lawful basis</u>	<u>5</u>
3. <u>What information?</u>	<u>6</u>
a/ Different types of information	6
b/ Information we ask you to provide or that is provided on your behalf	6
c/ Information that a Practitioner creates or records about you	7
d/ Information you may choose to provide to a Practitioner or to us	8
e/ Other Platform usage information that is collected by us	8
4. <u>Why & how information is used</u>	<u>8</u>
a/ Extent of our access and use	9
b/ Our prime purpose	9
c/ How do we do this?	9
d/ Ancillary to our main purpose	9
e/ How do we do that?	9
f/ Anonymous and Aggregated	10
5. <u>Disclosure & Consent</u>	<u>10</u>
a/ With whom we share	10
b/ Competing reason to disclose	10
6. <u>Practitioner as independent Data Controller</u>	<u>11</u>
a/ Restricted access	11
b/ Records	11
7. <u>Who uses information?</u>	<u>12</u>
a/ Data Controller/s	12
b/ Third party Data Processors	12
c/ Other types of access	13
8. <u>Security</u>	<u>13</u>
a/ Authentication	13
b/ Data Transfer	13
c/ Storage	13
d/ More information	13
e/ Your responsibility	13
f/ No guarantee	13



9. <u>Your access to and rights over your Personal Data</u>	14
a/ Your rights	14
b/ How to exercise your rights	14
10. <u>Complaints</u>	15
11. <u>When we no longer hold your data</u>	15



1. About us and contact details

We are ProblemShared, which is the trading name of Teledoctor Ltd, registered in England with company number 10410380 and at registered address 3 Frederick Street, London WC1X 0ND.

We provide access to mental health care services via our digital platform problemshared.net (the "Platform"). This encompasses a network of mental health practitioners (each a "Practitioner") who provide a range of services remotely, including via video link, to users of the Platform such as you.

As such we are a Data Controller for the purposes of the Data Protection Legislation, and the data that we handle that relates to you also includes Special Category or Sensitive Data in reference to your mental and physical health and any information that you opt to share with us based on gender, linguistic, ethnic or cultural preferences connected with therapy. This document further addresses our role, your data and your rights in relation to that.

If you wish to contact us regarding privacy and your Personal Data, please contact our Data Compliance Officer care of the following email address: help@problemshared.net

2. Lawful Basis

Legally we must have a lawful basis to access and use your data, and we must keep it private, and where that data does not remain private, it must only be where we are required or permitted by law to disclose it.

Before you book a Session with one of our Practitioners or you receive any service through our Referrals or Assessment Pathway, we ask if you have read and will consent to the terms of this Policy and to our User Terms and Conditions that are notified to you on our Platform under the relevant menu item. Consent is a lawful basis for the handling and processing of Personal Data. (Article 6a of the Data Protection Act 2018 "DPA").

Consent is not the only lawful basis on which we handle your Personal Data. And for data that includes Special Category Data or Sensitive Data, Data Controllers must have two lawful bases.

These bases are as follows. We handle your data on the basis of giving effect to contractual obligations (Article 6b of the DPA) such as those agreed by you with us in the Platform's User Terms and Conditions for us to provide you with access to health care, and between us and any Partner Organisation if you have been referred to us by them through the Referrals or Assessment Pathway and to give effect to any agreement you have with a Practitioner (these are singly and collectively referred to as the "contractual basis").



And we handle your data specifically for the purpose of providing health care (Article 9h DPA) ("healthcare basis").

Where we handle or process data (in the ways set out in this Policy) for a purpose that is not strictly either on a contractual or healthcare basis, we shall rely on your consent to this Policy to do so (Article 9a DPA). Where this is the case, it is specifically identified to you in the relevant section of this Policy (see Section 4f). In that instance, you are also able to withdraw your consent later should you wish to do so. In matters that are strictly contractual and healthcare related, we are unable to provide our service without being able to handle or process your data in the ways set out in this Policy because we would fall short of the duty expected of us in complying with our contractual obligations, and of our duties in facilitating your health care by Practitioners.

3. What information?

a/ Different types of information

Personal Data is defined in the Data Protection Legislation as information which, whether on its own or in combination with other information, allows for the identification of an individual. As noted earlier, some information may also be Special Category or Sensitive Data. Where personal identifiers are removed from the information during processing, for example the information is anonymised and then aggregated, this is no longer Personal Data.

There are different contexts in which we hold information about you. These are associated with discrete, albeit related, purposes, and are also associated with different mechanisms for control by you. We first set out each of the different contexts for information, next we describe our purposes in more detail, and then we address sharing and access to data, the relationship with your Practitioner, processing of data, your rights and when we no longer hold your data.

b/ Information we ask you to provide or that is provided on your behalf

We ask you for certain information when you sign-up or are enrolled on our Platform. This may also be information that is provided on your behalf, if you have come to us via the Referrals or Assessment Pathway. In this instance, we rely on the Partner Organisation or 3rd party who refers you to have in place your understanding and/or consent to such sharing of your personal data for example via their own Privacy Policy or Notice.



This includes:

i/ your full name, date of birth, email address, mobile telephone number and physical address which we use to identify you, to create a Booking or arrange a Referral or Assessment, and to contact you in relation to your use of the Platform or service you receive, or for safeguarding and this information is stored in your digital Health Record - this is mandatory;

ii/ your GP's name and GP practice contact details to further identify you and your primary health carer in case we need it for safeguarding purposes - this is mandatory;

iii/ an emergency contact in case of emergency or safeguarding - this is mandatory;

iv/ information connected with why you wish to see a Practitioner, and your medical history (which you may choose to provide in as much or as little detail as you like), medications, previous therapy - this is mandatory;

v/ billing or payment information - but which we do not store and which is handled instead by our third party supplier Stripe but which is mandatory in order to effect payment;

vi/ personal preferences for therapy or choice of Practitioner based on gender, linguistic, ethnic or cultural preferences - this is not mandatory;

vii/ questionnaires, surveys or other assessment tools generated or licensed by us for you to complete alongwith any third party in connection with the Assessment Pathway - if relevant to your care, this is mandatory;

viii/ any feedback from you in the event that you participate in a survey of the Platform.

With respect to sign-up or enrolment, you will be guided and prompted in filling in any required information fields on our intake form over the Platform dashboard.

You, or the Partner Organisation that refers you to us, or the third party that completes any assessment-related questionnaire on your behalf is solely responsible for the truth, currency, accuracy and completeness of the information about you that is provided to us.

c/ Information that a Practitioner creates or records about you

With respect to counselling with a psychotherapist or clinical psychologist, your Practitioner has discretion as to whether s/he wishes to store the records and observations of her or his Sessions with you ("Notes") on our Platform or according to their own usual practices, outside of our Platform. This is for two reasons, i/ the Practitioner is a Data Controller in her



or his own right because of the decisions s/he takes in the course of providing therapy and care to you and ii/ the Practitioner is an independent health care provider.

d/ Other information that you may choose to share with your Practitioner or with us

With respect to counselling with a psychotherapist or clinical psychologist, outside of the Assessment Pathway, we do not store information that either you or the Practitioner choose to share with each other during the course of your Session, for example a document with suggested exercises as part of your therapeutic relationship via separate email. In the event that you and the Practitioner share a document or file by email that contains information that is personal to you, the Practitioner is the person who controls and stores that information for the purposes of privacy. In the same way, the Practitioner may make notes of their Session with you, and this information is also personal to you. We address this later in the policy since Practitioners also hold, control, handle or process your information in this regard.

The content of any communication between you and us, separate to your Practitioner, also contains information relevant to you. When you contact the Company by email, we keep a copy of that email.

e/ Other Platform usage information that is collected by us

Each time you visit the Platform, we collect the following information about your digital activity including but not limited to the following:

i/ device specific information: the type of device (mobile or tablet) you are using; temporary or persistent unique device identifiers (UDIDs), the I.P. address of your Device, your mobile operating system, the type of mobile internet browsers you use;

ii/ usage information: the full uniform resource locator (URL) clickstream to, through and from the Site (including date and time); menu items, or pages you viewed or searched for; page response times; download errors; length of visits to certain pages; page interaction information (such as scrolling, clicks and mouse-overs); actual duration of video-link consultation during any Session in minutes; recurrence of visits to the Platform; recurrence of Sessions that you book; methods used to browse away from one page of the Platform and another, and any phone number used to call us at ProblemShared.

4. Why & how information is used

We will use your information only as is legally permitted. We may interact with information that is personal to you in a number of ways or contexts: we receive or request data from you, we receive or request your consent or change of consent with respect to your data, we store



data, we handle and use it, we direct or permit others to handle, process or use it, we provide copies of it to you at your request, and we eventually delete it.

a/ The extent of our access and use: Legally we must have good reason to access and use your data, and we must keep it private, and where that data does not remain private, it must only be where we are required or permitted by law to disclose it. In handling data, it is important to note that when the data has been anonymised it is no longer personally identifiable.

b/ Our prime purpose in handling your personal information is to facilitate your mental health care, and to give effect to the terms and conditions that are agreed between you and us for your use of the platform (Platform User Terms and Conditions), any agreement for your care with a Partner Organisation, and to give effect to any agreement you make with your Practitioner. We provide a centralised platform over which Practitioners can serve the mental healthcare needs of clients such as you in a remote setting via video-link consultation, for counselling therapy and in connection with assessment for certain mental health conditions.

c/ How do we do this? This includes identifying you and how we can contact you; facilitating a Practitioner's understanding of your health history; your reasons for seeking treatment; previous medications etc; contacting you if needed; facilitating a consultation or Session between you and a Practitioner via video over the Platform, enabling therapy preferences, if relevant, providing access to payment means for Sessions managing any complaint you make, and otherwise communicating with you in relation to your use of the Platform, eg via email, and sending you automated reminders about your Bookings.

We may also use your contact details to send information about updates and features of the our Platform from time to time if you have opted in to receive that. We do not and shall not enable third parties to market to you.

d/ Ancillary to our main purpose of providing a remote mental health care service via our Platform is the improvement and further development of the Platform itself, for the mutual benefit of the Company, Practitioners and Clients such as you to deliver a mental healthcare service that is user-friendly, secure, helpful, informed and responsive.

e/ How do we do that? We use information about how and why the Platform is accessed for our own analysis of efficiencies and operations of the Platform and to understand the incidence and expression of mental health in the community and our capacity to respond to that.

So we may also use data that is collected regarding devices and usage of our Platform for various technical reasons, such as troubleshooting, improving operations, and efficiency, statistical analysis, research, and survey purposes for Platform and service optimisation, and to monitor security of the Platform and protect against inappropriate or unpermitted use of



the Platform as per our User Terms. You may know this as "Cookies "and similar technologies that can be used to collect this information. You have the choice of accepting our cookies or not each time that you use our Platform.

On a broader level, we may also use data that informs about patterns and presentation of mental health matters to better inform our approach to providing more tailored and representative services.

f/ Anonymous and Aggregated: On both levels, analysis is carried out once we have first anonymised the data by removing all personal identifiers, and then aggregating or combining it with other amounts of data which means that, at that point, the data no longer constitutes personally identifiable information about you and may be mixed with lots of other anonymised information. This is a type of processing for which we would like your consent and if you agree to the terms of our Privacy Policy, you are showing your consent to us being able to anonymise and aggregate your data for the purposes set out above. You may withdraw your consent for processing for these purposes at any time by writing to us at: help@problemshared.net

5. Disclosure & Consent:

We must also obtain your consent first before we disclose any personally identifiable information to any other third party (separate to the processing that we may undertake under c/ above and as set out under section 7b below).

a/ With whom we share: We may share your information with your G.P. in case of any safeguarding concern. For this we do not need your consent. Otherwise, your Practitioner or we will ask to share information with your G.P. only with your consent or on your request.

If you are a client whose health care is supported by a Partner Organisation then we need to share with that organisation certain matters in connection with your mental health care including the name of your treating practitioner, the number of Sessions booked and attended, information in connection with appropriate safeguarding, outcomes including either in relation to an Assessment or a Practitioner's recommendation for concluding or advancing further Sessions, in order to facilitate your care on the terms which we are contractually obliged to so provide.

b/ Competing reason to disclose: If we disclose personally identifiable information about you without your consent then we can only do so where our action is necessary by way of a legal claim, or is required by any enforcement or other government agency, or as is necessary under any competing law or regulation, for example a public health interest, as may be required for any audit of service, including by reason of our registration with the national English health regulatory body, the Care Quality Commission (C.Q.C.) with respect to medical care, or in case of emergency or for the purpose of safeguarding you or another



person from harm, or to investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of our services. And the information disclosed would only be to the extent necessary and relevant to the purpose for disclosure.

6. Practitioner as independent Data Controller

The Practitioner you see in your Session or who is involved in your care or assessment is also bound to follow and comply with all relevant laws about privacy, like us. And if you are receiving counselling, including via any Referrals Pathway, the agreement you make with them in defining your therapeutic relationship should also address your rights and the Practitioner's obligations about privacy in connection with the information that they handle, hold and store about you.

a/ Restricted access: Only the Practitioner or Practitioners who treats you or assesses you has access to your digital Health Record in full. If you have been treated by more than one Practitioner, only the Practitioner currently treating you will have current access to this record.

Practitioners are not only bound by strict confidentiality practices to maintain your privacy, as per their relevant professional body's code of ethics, but also bound by compliance with the Data Protection Legislation by reason of their registration with the I.C.O as a Data Controller and their contractual agreement with us in which we also oblige them to do so too.

b/ Records: Depending on which type of client a Practitioner is treating, for example a self-referring client or a client of the Referrals Pathway for counselling, the Practitioner may choose to make their own arrangements with respect to certain matters such as storage and filing of Session notes or they may avail themselves of our Platform to store this; in any case, they are obliged to ensure that should they choose to store any data outside of the Platform, that they do so in keeping with good industry practice and in compliance with the Data Protection Legislation. Practitioners who are treating clients of the Assessment Pathway are obliged to keep all notes and records on the Platform.

With regard to recordings of any session, we note that there is no opportunity for any recording to be made over our Platform for privacy reasons. Should there be any request by a Practitioner to record a Session with you by some other means for some reasonable purposes connected with therapy, this must be evidenced in writing as agreed between you and the Practitioner as proof of your consent, alongwith provisions for the purpose and format of such recording, use, processing, handling and storage and deletion, as would be usual for privacy law requirements and must be included with your Health Record.



7. Who uses information?

a/ Data controller/s

i/ **Us:** For the purposes of the Data Protection Legislation, we are a registered Data Controller and we have a Data Registration Number with the UK supervisory body - the Information Commissioner's Office (I.C.O.)

ii/ **Your Practitioner:** As noted above, a Practitioner also has access to, stores and handles information about you. That Practitioner must also be registered with the I.C.O. for the same purposes as us.

iii/ **Partner Organisations** via the Referrals or Assessment Pathway (including for Supported Students for Subsidised Sessions) with whom we share certain information such as that listed under section 5 above. In this instance we agree in writing with the Partner Organisation those matters that will be shared and how we will share that information so that we comply with the Data Protection Legislation.

b/ Third Party Data Processors

We use other companies to provide data processing services on our behalf, for a range of purposes connected with your health care and giving effect to our agreement to provide a service to you, including facilitating the integration of parts of the Platform, enabling video-link consultations, storage and retrieval of your information, facilitating payment for Sessions, optimising functions of the Platform, analysing access to and engagement with the Platform.

With regard to personally identifiable information that enables payment for services, we do not store any such information. The third parties who are our suppliers of billing and payment function systems, credit checking or encrypted security solutions must be compliant with Level 1 Payment Card Industry (PCI) data security standards. Any payment transactions are encrypted using SSL technology.

Transfers of Data for processing purposes: We have in place agreements with our Data Processor/s that accord with Data Protection Legislation. Our Platform is only stored on U.K. based servers. Where we do share information with third party Data Processors, this will not be processed via destinations outside the European Economic Area unless it is in accordance with the protections afforded by the Standard Contractual Clauses of the Data Protection Legislation for such transfers that comprise as follows: the Data Subject has enforceable rights and effective legal remedies; and that the Party complies with its obligations under the Data Protection Legislation by providing adequate levels of protection to any Personal Data that is transferred, and that it obliges each Party to so oblige any Data Processor it appoints by providing for the same in its agreement with such Data Processor.



c/ **Other types of access** - As noted earlier, the Company may be required to provide information to others in the context of legal, enforcement or other governmental obligations.

8. Security

We take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of your Personal Data and against accidental loss or destruction of, or damage to, your Personal Data as required by the Data Protection Legislation. The Company has security measures in place and we contractually oblige our Data Processor/s, and any joint Data Controller with whom we may share information to provide for the same if relevant.

Some of these measures include:

a/ **Authentication** – confirmation of username and password and as may be required or adopted: 2 factor authentication.

b/ **Data Transfer** – Data in transfer is fully encrypted using the most secure cryptographic technologies available (256-bit level of encryption).

By encrypting electronically transmitted information such as video calls or messages, this information can only be accessed by the participating parties. With encryption, the rest of the information is distorted and unreadable, impossible to interpret without special keys.

c/ **Storage** – All information is stored on secure servers which have achieved the highest level of security certification and are located in UK-based data centres.

d/ **More information** - If you require any more information about the security measures we take in carrying out our obligations under the Data Protection Legislation, please contact our Data Compliance Officer care of help@problemshared.net

e/ **Your responsibility** - It remains your responsibility to ensure no-one else uses the Platform in your place, or gains access without your permission, and you are responsible for keeping your access private.

f/ **No guarantee** - Of course, no data transmission over the internet can be guaranteed to be 100% secure. While we undertake, in line with good industry practice, to protect your Personal Data, from unauthorised access, use or disclosure, we cannot ensure or warrant the security of any information you transmit via the Platform, including during any Session including from any Distributed Denial of Service attacks DDOS.



9. Your access to and rights over your Personal Data

a/ Your Rights

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a “Data Subject Access Request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

b/ How to exercise your rights

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, request the restriction of processing or request that we transfer a copy of your personal information to another party, please email our Data Compliance Officer care of: help@problemshared.net

You will not have to pay a fee to access your personal information (or to exercise any of the other rights) on the understanding that such is not vexatious.

To withdraw your consent to us anonymising and aggregating your data for the ancillary purpose of analysis of health care service capabilities and response, as cited above at section 4, please email our Data Compliance Officer care of help@problemshared.net



Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

10. Complaints

You may contact us regarding any complaint at help@problemshared.net

Alongside your right to contact us to make a complaint or other request with regards to your privacy, you may also contact the I.C.O. as follows: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, telephone: 0303 123 1113 (local rate).

11. When we no longer hold your Personal Data

We hold information personal to you for a period of seven (7) years after your care or treatment via our Platform has ceased including when your therapeutic relationship ends with a Practitioner or the date of your last Assessment.

With regard to medical records pertaining to psychiatric-based treatment over the Platform, we hold that part of your record in accordance with national best practice guidance as issued by the British Medical Association, Department of Health, and/or relevant NHS codes.

Type of record	Retention period
Records relating to persons receiving treatment for a mental disorder within the meaning of mental health legislation	20 years after the date of the last contact; or 10 years after the patient's death if sooner.

When it comes time to dispose of or destroy information personal to you we shall do that by secure means in line with good industry practice and in compliance with Data Protection Legislation.

But of course, we may retain Personal Data for other periods as mandated by any other Law which may requires us to do so from time to time.

