Contact tracing - protecting customer and visitor details

Share(Opens Share panel)

We understand that organisations have lots of new measures to put in place so that they can re-open safely to the public. For many, this includes collecting customers' and visitors' personal information for the first time, to support the various contact tracing schemes in the UK.

It doesn't need to be complicated - there's no need for you to develop special apps or digital solutions – just choose the process that best suits your business.

Follow our five simple steps to help ensure that data protection is not a barrier to your recovery.

A

Ask for only what's needed

You should only ask people for the specific information that has been set out in government guidance. This may include things like their name, contact details and time of arrival for example.

You should not ask people to prove their details with identity verification, unless this is a standard practice for your business, eg ID checks for age verification in pubs.

B

Be transparent with customers

You should be clear, open and honest with people about what you are doing with their personal information. Tell them why you need it and what you'll do with it. You could do this by displaying a notice in your premises, including it on your website or even just telling people.

If you already collect customer data for bookings, you should make it clear that their personal data may also be used for contact tracing purposes.

C

Carefully store the data

You must look after the personal data you collect. That means keeping it secure on a device if you're collecting the records digitally or, for paper records, keeping the information locked away.

See our guidance on simple security measures you can take here.

D

Don't use it for other purposes

You cannot use the personal information that you collect for contact tracing for other purposes, such as direct marketing, profiling or data analytics.

E

Erase it in line with government guidance

You should not keep the personal data for longer than the government guidelines specify. It's important that you dispose of the data securely to reduce the risk of someone else accessing the data. Shred paper documents and permanently delete digital files from your recycle bin or back-up cloud storage, for example.