

Data sharing code:

the basics



Sharing data can make life easier, more convenient and connected for us all, both at home and at work. If done under the right circumstances and for the right reasons, sharing personal data about someone with another business or organisation can help protect them or give them a better service.

There are various reasons why you may need to share information about people with others. For example, if you're a plumber, you might want to explain that you'll only keep your customers' details while your own guarantee lasts, and that you'll need to share their details with the manufacturer if they also want the manufacturer's guarantee.

The data sharing code of practice provides guidance on how organisations can share data in a way that is: accountable, lawful, fair, and secure.

Accountable

You're responsible for your compliance, and you must be able to demonstrate it.

Whether you have staff or trade by yourself, you're responsible for protecting the personal data of (or information about) anyone who comes into contact with you – including your customers, suppliers and staff.

You also need to demonstrate accountability. This means assessing the risks you create, taking appropriate action to minimise them, and being able to demonstrate your compliance.

Ways to demonstrate accountability when sharing data include documenting your decisions for sharing it and having a data sharing agreement in place. You also need to document when and how you'll delete data securely when it's no longer needed.

- [Make your own privacy notice](#)
- [Getting started with data protection – top tips for beginners](#)
- [What should be in a data sharing agreement?](#)

Lawful

You have to have a lawful basis for sharing data, and you should document this.

You can use [our interactive tool](#) to help you choose which lawful basis is most appropriate, depending on the reason you want or need to share the personal data. [Consent isn't always necessary or appropriate.](#)

Make sure you choose your lawful basis carefully because it can be difficult to change your mind after you've started using or sharing people's data, and you would need a good reason.

You'll also need to document what lawful basis you're using, say why you're using it, and tell people about it in your privacy notice.

You can [contact us for more advice](#).

- [How does data sharing apply to acquisitions and mergers?](#)
- [Can I share personal data with the police or other law enforcement authority?](#)
- [Can I share data in an emergency?](#)

Fair

If you're sharing people's personal data, it must always be fair as well as lawful.

This means you should only share their data in ways they'd reasonably expect. For example, if you've got their data through means that are misleading, then everything you do after that (whether you think it's lawful or not) is unlikely to be fair.

You need to make sure you're asking the right questions about any data that is supplied to you or that you intend to share, including the transfer of databases or lists between clubs, societies, charities, voluntary groups and political parties, for example. It doesn't make any difference whether it's for profit or not – if you intend to use it or share it, you're responsible for making sure it complies with the law.

- [The benefits of data protection laws](#)

Secure

You have to look after people's data and put measures in place to keep it from getting lost, damaged or stolen.

.....

Check your [security measures](#) line up with the sensitivity of the data you hold. The measures you choose are up to you but could include things like locking filing cabinets and putting strong passwords on your devices.

When sharing personal data with other businesses or organisations, choose a secure online document sharing system or a secure messaging app. If you have to use email, which is not always secure, consider password protecting documents and sharing the passwords via a different channel, like text. You should also:

- let the others know the nature and sensitivity of the information you are sharing with them;
- check with them if they have security measures in place; and
- agree on a set of security standards in a data sharing agreement, if you have one.

You could undertake a Data Protection Impact Assessment (DPIA) when planning on sharing data, so you can consider any security issues and how you will mitigate them.

- [Understanding and assessing risk in personal data breaches](#)
- [As a small organisation, do I need to do a DPIA?](#)
- [What is a data sharing agreement?](#)
- [11 practical ways to keep your IT systems safe and secure](#)

.....

When you get data protection right, it sends a strong message to your customers – it lets them know that you value and care about their information, and that you're more likely to keep it secure and not share it inappropriately.

The ICO is here to help. If you need more information or guidance on how to share data lawfully, go to ico.org.uk/datasharing

.....