



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Sharing Personal Information: Our Approach

Introduction

- This paper explains the Information Commissioner's general approach to information sharing. It does not provide detailed compliance advice. It is aimed primarily at public bodies.
- Information sharing should be supported by a sound business case, preferably accompanied by a Privacy Impact Assessment. This should identify the intended benefits and demonstrate that the data protection risks have been identified and addressed.
 - The **benefits** may arise for society as a whole or for the individuals directly affected;
 - The data protection **risks** are those which involve intrusion into personal privacy or which threaten the integrity of the personal data.
- We expect the sharing of personal information to be justified on the basis that the benefits – supported by meaningful safeguards – clearly **outweigh** the risks of negative effects. Where sharing is justified all reasonable steps should be taken to keep any negative effects to a minimum.
- This approach means that when seeking the benefits of sharing personal information, organisations must ensure protection for the people the information is about. Data protection law provides a framework to help organisations strike this balance correctly. In striking the balance:
 - ICO expects public bodies to remain within the boundaries of the **reasonable expectations** of those affected and to be mindful of the **adverse reactions** they will encounter if they share information in ways which forfeit public trust and confidence.
 - ICO will **avoid an overly restrictive application** of data protection law where that would lead to organisations failing to make sensible use of the information they hold;
 - ICO recognises that modern information technology allows the sophisticated analysis and rapid transmission of information. Our approach will not prevent public bodies making the most of the benefits that technology can bring to society and individuals. It will enable them to fulfil their responsibilities and provide services to **standards the public expect**.

Threats to privacy and integrity

- Our starting point will be to look at the effect of information sharing on individuals. If there is no risk of real unfairness or unwarranted detriment, we will not seek to use our powers to prevent the sharing. By 'detriment' we mean not only material loss or damage but also less tangible damage, distress or embarrassment. We recognise that in some cases some detriment may be warranted, for example where information sharing leads to a fraudulently claimed payment being stopped.
- We expect organisations to adopt a privacy-friendly approach, e.g. avoiding or minimising the use of information in a form that identifies people. For example, for planning purposes it may only be necessary to know how many people of a certain age group live in a particular area. In such cases only statistical information should be shared. The amount of information shared, and the extent of sharing, should be limited to that necessary to carry out the initiative.
- The threshold for sharing sensitive or confidential information is higher than that for other sorts of information. Some information, for example that relating to a person's health is considered particularly sensitive and most people would probably expect their consent to be obtained prior to it being shared. The sensitivity or confidentiality of personal information will be reflected in our approach.

Choice and consent

- We expect individuals to be able to exercise choice to allow their information to be shared wherever this makes sense. However, where consent is used as a basis for information sharing, it should be a genuine free choice for the individual. Consent should not be used to legitimise initiatives where, in reality, the individual has little or no choice. In many circumstances the individual's consent is not the best basis for sharing personal information.

Transparency and Information

- We expect a high degree of transparency when information is being shared. This means taking active measures to inform people how information about them is being used and whether / how it will be shared. Organisations should use simple, clear and informative fair processing notices. We will also encourage public bodies to put documents about their information-sharing practices in their freedom of information publication schemes.
- We will use our powers to ensure that individuals' legal right of access to information about themselves is always upheld. However, we will also encourage organisations to go beyond simply meeting their legal

duties by developing cheaper, better ways of giving people access. The technology that supports the sharing of information between organisations should also allow it to be made more readily available to the people it's about.

Quality and Security

- If organisations are going to share information they must have the capability and resources to ensure that its quality is good enough to support the use to which it will be put.
 - This might mean, for example, checking that information is up to date and recorded in a compatible format;
 - Particular care is needed to avoid false matches, or making unfounded inferences;
 - We expect measures to be taken to make sure inaccurate information is corrected by all the organisations with which it has been shared;
 - Where necessary we will take action to ensure that organisations involved in information-sharing pay due attention to information quality issues.
- We expect organisations sharing information to be able to demonstrate that they have addressed the technical and organisational security implications of doing so. In the context of greater information sharing we see information security as an increasingly important issue.
- Where the sharing of personal information poses a particular privacy or integrity risks, we expect counterbalancing safeguards to be put in place. For example, strict limitations could be placed on the use of the shared information and a suitably high level of security established.

Public law

- We will not normally investigate whether a public body's sharing of information complies with the wider elements of public law that apply to it. We will rely on the public body to make its own assessment that it meets the general requirements of public law. We will only consider wider public law aspects where there seems to be obvious breach or where there is a real likelihood of unwarranted detriment to individuals.