

# Data-sharing

## 1 Establish the basis to work together across the region

As part of setting up your recruitment support hub you will need to ensure you have a documented process for working with your regional partners. This should ideally take the form of a partnership agreement.

### Key elements for the partnership agreement to consider are:

- Clear, shared objectives and vision
- A realistic plan and timetable for meeting those objectives
- How the recruitment hub will operate, for example is it hosted by one of the partners or a separate legal entity. This will determine who is the data controller
- The structures, purpose, activities and exit strategy
- A clear framework of responsibilities, accountability and decision making powers and processes
- How the partnership will meet its agreed functions and how this will be achieved, for example shared funding, staffing, training

## 2 Map your data requirements

Data mapping is a useful for data protection impact assessments (DPIA) and helps to understand what data will be processed.

The regional partnership should:

- Map out the workstreams and data flows for each function of the recruitment hub
- Identify what data will be processed and what systems will be used
- Identify and assess any risks to individual's privacy
- Put in place measures to mitigate those risks
- Agree how the data controller/s will comply with UK GDPR individual rights
- Complete the DPIA and agree which partners will lead. You can use the ICO's DPIA template or agree to use a partner's template



[Information Commissioner's Office DPIA guidance and template](#)



### Achieving for Children

Before Achieving for Children implements any project that involves processing personal data they complete a Data Protection Impact Assessment (DPIA).

A DPIA is a risk assessment which addresses the use of personal data within proposed business processes and seeks to minimise the risks.

In line with their right to be informed, Achieving for Children communicate plans to the data subjects affected. This is important if data has been collected for another purpose. If the data subjects were not informed Achieving for Children would make a record of this decision and the reasons why within the DPIA.

If data is processed electronically or if data is collected using a new or existing case management system, Achieving for Children checks there are appropriate IT security arrangements in place.

Achieving for Children also considers whether other professionals, either internal or external, might have a stake in the data being processed and if their own processing might be affected as a result.

Achieving for Children ensures every decision is documented and signed off Data Protection Officer.



[Information Commissioner's Office guidance on Data Sharing](#)



[ICO Guidance on rights of individuals](#)



[ICO Privacy notice template](#)



[Achieving for Children privacy notice for fostering services](#)

# Data-sharing

## 3 Establish a data sharing agreement

Data sharing agreements set out the purpose of data sharing, outline what happens to the data at each stage, set standards for data sharing and help all the parties involved in sharing to be clear about their roles and responsibilities.

Having a data sharing agreement in place helps you to demonstrate you are meeting your accountability obligations under the UK GDPR.

The agreement should be written in clear, concise language that is easy to understand.



### Things you should consider in a data sharing agreement

- Who the parties in the agreement are
- Agreement ownership, review and termination arrangements
- What the purpose and benefits of the data sharing initiative is
- Which other organisations will be involved in the data sharing
- Are you sharing data with another controller
- What data items are you going to share
- What is the lawful basis for sharing information
- The special category data, sensitive data or criminal offence data being collected
- Arrangements for managing individual rights
- Approach to storing and handling information securely
- Data breaches and incident procedures

## 4 Key things to do

### Do:

- Involve your Data Protection Officer (DPO) from the outset
- Engage you Information Governance team from the outset
- Be realistic about the resources required to manage data protection responsibilities
- Use the [Information Commissioner's Office](#) website for guidance and templates
- Justify what information you will collect and how it will be used
- Make sure you are clear with data owners about how you will process their information
- Have clear procedures in place to manage individuals' data rights
- Make sure your case management system is safe and secure

### Don't:

- Forget to support your workforce to understand their data protection responsibilities
- Rely on others to meet data protection accountabilities

### Summary of steps

