# The Plymouth Alliance Information Sharing Agreement: Guidance for Partners

## Purpose of this Guidance

This document explains what The Plymouth Alliance Information Sharing Agreement (ISA) is, why it exists, what it allows organisations to do, and what it does not allow organisations to do.

It is intended to support consistent understanding and decision-making across Alliance partners and should be read alongside each organisation's own data protection policies, privacy notices, contracts and procedures. The ISA sits alongside these arrangements; it does not replace them.

## What is The Plymouth Alliance?

The Plymouth Alliance is a partnership of organisations working together to improve outcomes for people experiencing multiple disadvantage and complex needs, including homelessness, offending, poor mental health and substance use. Alliance partners include statutory, voluntary and housing organisations working together to coordinate support and improve services.

The Alliance recognises that no single organisation can meet all of a person's needs. Effective partnership working often requires organisations to communicate with one another and, in some circumstances, share information to provide safe, effective and coordinated support.

## Why Do We Have an Information Sharing Agreement?

The ISA provides a shared framework for responsible information sharing between Alliance members. It exists because partner organisations regularly work with the same individuals and may need to exchange information to:

- coordinate support;
- improve outcomes;
- reduce duplication;
- manage risk;
- safeguard individuals and others;
- support effective service delivery; and
- understand demand and service use across the Alliance.

The ISA establishes common expectations and standards for how information should be handled so that sharing is lawful, necessary, proportionate and secure.

The Plymouth Alliance

## What Does the ISA Allow Us to Do?

The ISA provides a framework that enables Alliance partners to share information when it is lawful and appropriate to do so. This **may** include information sharing:

- during joint work with an individual;
- when coordinating services between organisations;
- during multi-agency discussions;
- when managing significant risks or safeguarding concerns;
- when supporting transitions between services; and
- for agreed service monitoring and statistical purposes.

The ISA also establishes shared principles including:

- information should only be shared where necessary;
- information should only be shared for a legitimate purpose;
- information should be relevant and proportionate;
- information should be accurate;
- information should be handled securely; and
- only the minimum necessary information should be shared.

The ISA therefore supports informed decision-making about information sharing and gives organisations confidence that partners are working within a common governance framework.

## What the ISA Does Not Do

It is important to understand what the ISA does not do.

The ISA:

- does not create a blanket permission to share information;
- does not grant unrestricted access to another organisation's records;
- does not make all information held by one partner available to all other partners;
- does not replace professional judgement;
- does not override contractual restrictions;
- does not override confidentiality obligations;
- does not replace legal requirements under data protection legislation;
- does not replace individual organisations' privacy notices, policies or procedures; and
- does not remove the need to consider whether sharing is necessary and proportionate in each situation.

The Plymouth Alliance

Being a member of The Plymouth Alliance does not create an automatic right to access personal information held by another organisation.

Every sharing decision must still be considered on its individual merits and must be supported by an appropriate lawful basis.

## Who Is Responsible for Information?

Each Alliance organisation remains an independent Data Controller for the information it collects and processes. This means each organisation:

- decides what information it collects;
- decides why it collects it;
- determines how it is used;
- identifies the lawful basis for processing;
- remains accountable for compliance with data protection legislation; and
- is responsible for decisions about sharing information it holds.

No Alliance partner transfers these responsibilities to another partner simply by signing the ISA.

## What Does the Law Require?

Information sharing within the Alliance must comply with:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Human Rights Act 1998;
- Common Law Duty of Confidentiality; and
- any other legislation or contractual obligations relevant to the services involved.

The law does not prohibit information sharing. However, it requires organisations to ensure that sharing is lawful, fair and justified.

When considering sharing information, organisations should ask:

1. What is the purpose of the sharing?
2. Is sharing necessary to achieve that purpose?
3. Is there an appropriate lawful basis?
4. Is the information relevant to that purpose?
5. Is the amount of information proportionate?
6. Can the objective be achieved with less information?
7. Is the information being shared securely?

The Plymouth Alliance

## What About Consent?

Consent is one lawful basis for processing information, but it is not the only lawful basis.

Depending on the circumstances, information sharing may be carried out under other lawful bases where permitted by law, including public task, legal obligation, vital interests or legitimate interests, depending on the organisation and the service being delivered.

Individual organisations remain responsible for determining which lawful basis applies to their own processing and sharing activities.

## Responsibilities of Alliance Partners

All Alliance partners are expected to:

- maintain appropriate data protection policies and procedures;
- provide staff training on confidentiality and information governance;
- ensure privacy information is available to service users;
- keep information secure;
- share information only when lawful and necessary;
- maintain accurate records of sharing decisions where appropriate;
- report and manage data breaches;
- cooperate with partners where information governance issues arise; and
- regularly review their own information governance arrangements.