



Horsham  
District  
Council

# Information Security Policy Suite

## Information Sharing Policy

### ISPS-008

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Technology Services Management Team, to obtain a copy in a different format.

## 1. Purpose

Information (Business data) sharing across and between organisations, under the right circumstances and for the right reasons, can play a crucial role in providing a better, more efficient service to customers. Without understanding what can and cannot be done, we are as likely to disadvantage our customers through excessive caution as we are by carelessness. The Council wants its customers to benefit from responsible sharing of data, confident that their personal data is being handled responsibly and securely.

The purpose of this policy is to establish the Council's approach to all types of data (information) sharing and provide a framework so that it can share information appropriately in accordance with relevant legislation and individual's rights.

## 2. Scope

This policy applies to all staff, members, contractors and any other persons who have access to the Council's information, information systems and networks.

This policy applies to all data (information) held, created, modified or accessed from the approval date of this policy. It includes data (information) in any form, e.g. electronic or paper.

## 3. Policy Statement

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures that encourage good working practices in all areas of data (information) sharing. Where possible a Data Sharing Agreement should be in place, however there are circumstances where this is not possible. These are;

- Contract - the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation - the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests - the processing is necessary to protect someone's life.
- Public task - the processing is necessary for you to perform a task in the public interest

When sharing information, the Council must:

- a. Have regard for the Data Protection Act 2018, the Human Rights Act 1998 and the ICO's Data Sharing Code of Practice;
- b. Ensure that the data can be shared and then to be clear as to the best way of achieving this;
- c. Ensure that data (information) is shared with the right people on a 'need to know' basis only;
- d. Ensure information sharing protocols and data exchange agreements are in place and adhered to;
- e. Document whether sharing is on-going, routine or one off;

- f. Ensure when it shares data (information) that the recipient(s) understand the nature, sensitivity and protection applicable to the information;
- g. Review what data (information) it receives from other organisations, ensuring its origin is known and any conditions that are attached to it;
- h. Keep appropriate records of any data (information) shared or received.

### 3.1 Consent

- a. The Council must, where appropriate, gain consent from individuals before sharing their personal information, except where the Data Protection Act permits it.
- b. Where the information sharing concerns the safety and welfare of a child or vulnerable adult, or the sharing is covered by statute, legal proceedings or is necessary for the provision of an essential service, consent may not be required.

### 3.2 Privacy notices

The Council must ensure, where possible, that:

- a. Individuals are aware of the Legal purpose for which we collect their information and how it will be used;
- b. Appropriate privacy notices are in place and fully accessible, i.e. on the Web Site;
- c. All privacy notices should include the following as a minimum:
  - c.1. The reason we share information;
  - c.2. Who we share data with.

## 4. Responsibilities

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

Additional responsibilities arising from this policy are specified below.

### 4.1 Data Protection Officer (DPO)

The Council's DPO is responsible for providing advice to IAOs, staff and members in relation to:

- a. All types of information sharing;
- b. Controls and procedures required to support information sharing in practice.

## 5. Training associated with this Policy

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

## 6. Monitoring

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

### 6.1 Non-compliance

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

### 6.2 Review

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

## 7. Equality Impact Assessment (EIA)

As per [the Information Governance and Security Policy \(ISPS-001\)](#)

## 8. Related documents

This policy should be read in conjunction with the following documents:

- ISPS-001 Information Governance and Security Policy;
- Any agreed data sharing protocols;
- ISPS-011 Data Protection Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures.

## Appendix 1: Key Concepts

### 1. Data sharing

Data sharing is the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

- a. A reciprocal exchange of data;
- b. One or more organisations providing data to a third party or parties;
- c. Several organisations pooling information and making it available to each other;
- d. Several organisations pooling information and making it available to a third party or parties;
- e. Exceptional, one-off disclosures of data in unexpected or emergency situations;  
or
- f. Different parts of the same organisation making data available to each other.

Some data sharing doesn't involve any personal data, for example statistics that don't identify anyone. Although Data Protection does not apply to this kind of data sharing, it is mentioned here for completeness. Separate guidelines are issued to staff to cover this particular type of data sharing.

### 2. Types of data sharing

There are four main types of data sharing:

- a. Systematic - routine data sharing where data sets are shared between organisations for an agreed purpose. This will be pre-planned and governed by established rules and procedures.
- b. Ad hoc or 'one off' - sharing data that is not covered by any routine agreement. Often this is an emergency situation and professional guidance and ethical rules will be applied to this kind of sharing. Records will be kept detailing the circumstances, what information was shared and explaining why the disclosure took place.
- c. Sharing data with a data processor – this requires a written contract, that ensures the processor only acts on instructions from the data controller and that the processor has security in place that is equivalent to the that imposed on the data controller (the council).
- d. Sharing within organisations – requests for data from one department to another. An internal information sharing protocol will cover all internal information sharing.