



Data Sharing Policy

Updated: March 2024

To be reviewed: March 2025

Author: Andy Walker

**EQUALITY SCHEME
EQUALITY IMPACT ASSESSMENT FOR
DATA SHARING POLICY**

Staff / Committee involved in development:	Health Safety Committee; Headteacher
For use by:	Staff and Parent/Carers and Governors
This policy relates to statutory guidance:	Data Protection Act 2018
Key related Farndon Policies:	Data Protection Policy Retention Policy Data Breach Procedure Freedom of Information Policy

Equality Impact Assessment: Does this document impact on any of the following groups? If YES, state positive or negative impact, and complete an Equality Impact Assessment Form or action plan, and attach.

Groups:	Yes/ No	Positive/Negative impact
Disability	No	
Race	No	
Gender	No	
Age	No	
Sexual Orientation	No	
Religious & Belief	No	
Gender Reassignment	No	
Marriage & Civil Partnership	No	
Pregnancy & Maternity	No	
Other	No	

Reviewed by	Leadership and Management
Agreed by	Finance / Health Safety Committee Policies with negative impact must be notified at full governing body
Next Policy review date	March 2025

A copy of this form, and any related impact assessment form or action plan must be sent to the school office

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors

INTRODUCTION

It is important that we understand why we share information, how we do it and for what purpose. A key part of this is our data mapping which shows how we process personal data throughout the school and it is important in allowing us to understand the sharing of data.

Where we share information regularly with organisations such as the Council, Department for Education etc there are defined process in place and in most cases such sharing is covered by a data sharing agreement – a document that states the expectations in relation to what will be shared, when and how.

If we provide information to a data processor to allow them to undertake work on our behalf, this will be covered by contract or by a Data Processing Agreement.

Both Data Sharing Agreements and Data Processing Agreements are covered in a separate guide.

With one off or irregular requests to share information we may have no formal process in place and we then determine whether we can share, what to share and why.

It is important to remember that the GDPR is not designed to prevent us from sharing information, it is there to ensure when we do share, we do it appropriately.

Whether we do or don't decide to share, the decision is recorded for future reference should it be challenged at any point.

The ICO provide a checklist to guide us through the steps necessary to make a decision.

The Appendices contain a Data Sharing Request form for recording when requests are made and a Data Sharing Decision Form for recording the decision made to share or not.

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
 - Only share what is necessary.
 - Distinguish fact from opinion.
- How should the information be shared?
 - Information must be shared securely.
 - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent

Appendix 1

Data Sharing Request Form

All requests for the sharing of data must be recorded whether or not data is to be shared. Requests should be logged and passed to the school DP Lead.

Note: this form is not for the request of personal data by individuals; see the Subject Access Request Policy.

Name of organisation:	<i>Details of the organisation requesting information.</i>
Name and position of requestor:	<i>Identify the contact details of the individual making the request to determine if they have the authority to do so.</i>
Date of request:	<i>Date request was made</i>
Data Sharing Agreement:	<i>Is a data sharing agreement required or is one in place?</i>
Date requested	<i>Date of existing Data Sharing Agreement or date DSA requested.</i>
Purpose of request:	<i>Clearly detail what has been requested and why.</i>
Date required:	<i>Date when data would be required</i>
Specific arrangements in relation to security, retention or deletion of data:	<i>Detail any arrangements in relation to how data would be provided etc</i>
Signed:	<i>Signed by recorder</i>
Date:	<i>Date request recorded</i>

Appendix 2

Data Sharing Decision Form

To be completed to record incidents of the sharing of personal data. This form should be filed with the Data Sharing Request form and, where relevant, a copy of any Data Sharing Agreement.

Name of Organisation:	Organisation involved
Name and position of person requesting data:	Contact details of requestor
Date request received by DP Lead:	Date request was passed to DP lead for assessment
Data Requested:	What information has been requested
Purpose:	What is the purpose of the request, why does the organisation require the information
Decision:	Are you sharing the information?
Is a Data Sharing Agreement required:	Data Sharing agreements are required for the regular sharing of data or where a large amount of data is involved.
Details of Data Sharing Agreement:	If there is a DSA, what is the reference number
Data supplied:	What information is being supplied
Reason for disclosure or non-disclosure:	What is the basis on which the decision to disclose or not disclose based, what allows this to happen?
Specific arrangements regarding security, retention or deletion of data supplied:	How is the information being sent, is it encrypted, how long is it to be used, how is it deleted etc.
Decision taken by:	Name of authorising person
Date of disclosure:	Date information was/is to be shared.
Signed:	
Date:	