Moulsham Junior School

Sharing Data with Other People/ Organisations

Contents

1. Introduction 2
2. Quick Reference Guide 2
3. Policy References 3
4. Requests to access personal data under the subject access provisions of the Data Protection Act 2018 3
5. Sharing between Agencies to support service delivery 4
6. Engaging a supplier to store or process personal data on your behalf 4

Data Processors 4

Engaging new Data Processors 5

Data Controllers 6

7. Requests to share personal information with the Police or other similar organisations 7
8. Requests to share ad hoc personal information 8
9. Data sharing with volunteers, work experience students, PTA, after-school clubs etc 8
10. Advice and Support 9
11. Breach Statement 9

Annex A: Processors & Controllers 10

Annex B: The Scope of a 'Written Contract' 11

1. Introduction

The school is the Data Controller for the personal data it collects and uses to run its operations. This means the school must comply with data protection law, protect individuals' privacy, and ensure the security of the personal data. The school may be asked to share some of the personal data it processes in a variety of ways, for example:

1. A parent/carer, pupil or member of staff may request their own data (see detailed guidance in the SAR Procedure (F3) and see section 4 below
2. Another organisation may ask you to share data with them to support services for young people, for example health agencies may ask to share data for the purposes of vaccinations. This is most likely to be supported by a data sharing protocol. See the Data Sharing Protocol template (E5) and see section 5 below
3. You may employ the services of a supplier to process or store personal data on your behalf, for example your pupil management system, e.g., SIMS. You must have a contract in place to support this sharing, see Contract Schedules (E1 & E2) and see section 6 below
4. The police or other organisations may contact the school requesting information about a pupil or member of staff. Detailed guidance on how to handle such a request can be found in Request for Personal Data (E8) and see section 7 below
5. A member of the public may contact the school asking for information about a pupil or member of staff. Please see section 8 below
6. Members of the public may access your school site and have access to personal data, for example volunteers or student teachers. These people should sign a non-disclosure agreement (E6). For more information see section 9 below.

It is important to note that the sharing of personal data is an activity which can have great benefits, sometimes of vital importance to the welfare of data subjects, and there are continuing efforts to make this process easier in law. Whilst care should be taken to ensure that sharing is lawful and transparent, there should be no presumption that sharing of personal data on request is absolutely prohibited.

Let's look at each of the above scenarios in more detail to understand the requirements for each, and what should be considered before a disclosure is made.

2. Quick Reference Guide

- If you receive a data subject access requests (someone asking for a copy of their own data held by the school) ensure you follow the SAR procedure and comply with the statutory timeframe for responding to the request

- If you wish to share personal data with another organisation to support the delivery of services, you must ensure this is supported by a contract or a data sharing protocol or a memorandum of understanding. Whichever you use it must make clear the responsibilities of each party to the sharing, the reason for the sharing and the lawful basis on which the sharing takes place
- When procuring services involving the storage or use of personal data always ensure you have a written contract between parties, or other agreement which is legally binding on the parties
- When procuring services, or considering sharing data under a data sharing protocol, you must complete a Data Protection Impact Assessment (DPIA) to identify risks and mitigations to ensure sharing is lawful, safe, and fair
- If the police or another organisation, ask for personal data you must consider your responsibilities under data protection law and human rights law. Sharing can only take place where it is necessary, proportionate, and justifiable. Records must be maintained of any sharing of this nature
- If a member of the public requests access to personal information held by the school, perhaps about a specific individual, you can only share where you have an identified legal basis to do so, or where the data subject has consented to the sharing
- School visitors who will have access to personal data, e.g. volunteers, must sign a non-disclosure form.

3. Policy References

This procedure is a requirement of the Data Protection Policy

4. Requests to access personal data under the subject access provisions of the Data Protection Act 2018

Individuals have the right to request access to their personal data being processed by the school. Requests to access personal information under the access provisions of the Data Protection Act 2018 must be responded to within one month of receipt. Requesters do not need to mention the Data Protection Act, it is for the school to recognise which legislation should be referred to when processing requests for information.

Generally, individuals are only able to request access to their own personal data, however where a child is under the age of 12 or where they lack capacity to understand this right, it can be exercised by those who have parental responsibility for them. For more detailed information on processing these requests, please see the SAR procedure (F3).

Required Actions:

- Ensure staff are trained to recognise requests made under the data protection act for an individual's personal data. Ensure staff know who to pass these requests to for processing
- Ensure designated staff have access to and understands the SAR procedure and how requests must be processed

5. Sharing between Agencies to support service delivery

When sharing with other Data Controllers you must be able to justify why you are doing so. Schools regularly share personal data with the DfE, the Local Authority, and the NHS. There should be existing agreements in place which provide you with the necessary documentation to make the sharing legally sound. Complaints about your sharing data in this way can be resolved by presenting an Information Sharing Protocol to the complainant.

Where you are proposing to enter into agreements to regularly share data with other organisations not covered by an existing Protocol, the parties proposing to share need to establish a Sharing Protocol (using the template at E5) and a DPIA should be completed. Once established, the sharing needs to be conducted in line with the provisions agreed in the Protocol. It should also be published for transparency.

Data sharing agreements (ISPs) must be regularly reviewed to ensure that they are still required, and that no changes have been made to the purpose or process, or to the legislation which may underpin the sharing.

Required Actions:

- Complete a DPIA to assess any risks the data sharing may create
- Draft or sign up to an appropriate ISP which sets out why, how, when and under what conditions data will be shared
- Ask WEISF@essex;gov.uk to publish any ISPs on their website to meet your transparency obligations and prompt reviews of the ISP
- Review ISPs when prompted to ensure they remain necessary and fit for purpose
- Ensure all ISPs are refenced in your RoPA for the relevant data flow
- Ensure the data sharing activity is referenced in privacy notices
- Record the ISP on the B1 Reporting Tool

6. Engaging a supplier to store or process personal data on your behalf

Data Processors

When a Data Controller uses a Data Processor to deliver services which require handling or storing personal data, the law makes clear that the Data Controller is still

legally responsible for that data and that the Data Processor can only act on the Data Controller's instructions under a 'written contract'

In practice, a 'written contract' can be a contract provided by the Data Controller for the Processor to sign, or it can be a Contract/ Agreement/ Terms & Conditions provided by the Processor for the Controller to agree. If it is the latter, then the Controller has a clear responsibility to make sure that 'contract' provided to them meets the requirements under the law. This can be achieved by comparing the information schedule of the contract with the contract schedule E1 and ensuring that all elements in the school's contract schedule are covered in the one provided to them. If this is not the case, you should ask the supplier to also sign your contract schedule to assure the legality of the processing.

The principle that the law introduces is this:

- A contract is a legal requirement of the Data Protection Act 2018, which applies the General Data Protection Regulations (GDPR)
- If the Controller fails to have a data protection compliant contract with a Processor in place, then the Controller is liable for any data breaches by the Processors whilst processing your data.
- However, if the breach related to an activity which the Processor had committed in the Contract to preventing, then the Processor has acted outside of the contract and has become the Data Controller in that instance.
- Regulatory action (including monetary penalties) is taken against Controllers. The Processor, by becoming the Controller could therefore be liable for any regulatory action instead of you.

This is the benefit of having a comprehensive written agreement underpinning the services provided to you by a Processor.

You must identify what could currently constitute a 'written contract' in each instance of a procured service which involves the storing or using of personal data. This could be a formal contract, a copy of the Processor's 'Terms & Conditions,' other information available on their website such as a Privacy Policy/ Statement or a Data Protection Policy/ Statement. You should keep this documentation for all your Processors in an Evidence File (or collection of files) for ease of review.

The General Data Protection Regulation (2016) (GDPR) sets out in Article 28 what the law would expect such a 'written contract' to cover (see Annex B). You should therefore review your Evidence File for each Processor against these requirements and make a conclusion about whether the evidence is sufficiently detailed to satisfy your needs under the law.

Engaging new Data Processors

When you are planning to engage with a new Data Processor either to deliver a service to you or to provide you with a system which involves them storing or being

able to access personal data, you will need to ensure that the 'written contract' is in place. Firstly, you will need to consider what assurances you are going to need from the Supplier to be confident that they comply with the law.

Certain processing requires you to complete a Data Protection Impact Assessment (DPIA) (Document G4). Previously known as a Privacy Impact Assessment and recommended as good practice by the Regulator (the Information Commissioner Office (ICO)), GDPR now requires these to be undertaken by law if your proposed processing poses "a high risk to the rights and freedoms of" data subjects (Article 35).

The term "high risk" is not well defined in the law, but as a rule of thumb, wherever your proposed processing involves Special Category (sensitive personal) data, then undertaking the DPIA process is advised. The process is a risk assessment, prompting you to consider how your new service or system is going to remain compliant with the law. Use document G5 to guide you through the risk assessment.

A DPIA is a legal requirement in the following circumstances:

- New technologies or changes to existing technologies
- Processing genetic or biometric data
- Systematically monitoring publicly available areas e.g., CCTV
- Transferring or hosting data outside the UK
- Intention to match or combine datasets from different sources
- Processing which may endanger physical health or safety in the event of a breach e.g., safeguarding or child protection
- Tracking individuals' location or behaviour e.g., Apps which hold location data
- Profiling children or targeting marketing or online services at them
- Profiling individuals on a large scale

It is advisable to engage with your Data Protection Officer (DPO) as early as possible in this process as the law requires the School to seek the DPO's advice. There should be evidence of the DPO's involvement, e.g., an approval 'sign-off' to satisfy the legal requirement.

The Supplier Security Questionnaire (Document G7) can be used to gather information from a potential supplier to assure that they can process your data securely and in line with legal requirements.

Where you have considered a new processor and decided that the activity does not need a DPIA, then there should be a record of this in case of challenge. The DPIA form (Document G4) allows you to capture these decisions.

Data Controllers

There will be occasions where you will need to share some personal data with a professional service provider, for example Educational Psychologists, and for those

occasions you should have a contract in place. A template contract for Data Controller to Data Controller can be found in the IGS framework, document E2.

Required Actions:

- Complete a DPIA to identify any risks
- Ensure you have an appropriate contract in place which meets the legal requirements
- Ensure contracts are referenced on your RoPA
- Ensure your RoPA documents any processing your suppliers may do outside the UK and the safeguards relied on to protect the data and data subjects' rights
- Create and maintain an evidence file for each supplier to hold any risk assessments, evidence provided as part of the procurement exercise and the contractual documentation
- Regularly review your supplier's performance against your contract to ensure their processing meets the contractual terms

7. Requests to share personal information with the Police or other similar organisations

You may be approached by organisations from time to time asking to share data on an ad hoc basis. Conversely, you may wish to approach another Data Controller to ask them for their data. In any event it is the responsibility of the Controller requesting the data to explain how this may be done in line with the law (i.e., what provision in the Data Protection Act 2018 allows them to have the data), and the Controller who owns the data to consider their request. For example, the Police wanting CCTV recordings or access to Child Protection data would need to confirm that the information is required for a criminal investigation.

The law does not require you to provide the information. It is for the Data Controller to consider the request and make a judgement whether they believe it is necessary, proportionate, and justifiable in the circumstances. If you refuse to provide the information the police can still apply to the Courts for access to it if they wish. If a Court directs disclosure, it is no longer the Data Controllers responsibility to consider the risks of disclosure as it has become a legal requirement.

You should seek advice from your Data Protection Lead before disclosing data as the disclosure must be approved and logged to ensure that the school can evidence due diligence was done in the event of a complaint. Please see guidance in document E8.

Required Actions:

- If a request is received, ask the requester to complete document E8
- Consider whether the requester has provided you with the signed consent of the data subject

- Consider the reasoning provided for requesting the data, and the personal data requested, and then decide if you as Data Controller believe sharing this data is necessary, proportionate, and justifiable in the circumstances
- Complete the bottom section of E8 to capture your decision regarding disclosure and your rationale for making that decision
- Record the request and the outcome on your B1 reporting tool

8. Requests to share ad hoc personal information

Privacy is everyone's right under the Human Rights Act 1998. The law does allow the sharing of personal data without consent in certain limited circumstances, for example if someone is at risk of serious harm or the law requires you to share the information. More commonly though, you will need the consent of the individual to share their personal data. Where consent is sought for disclosure, you must ensure that the consent is:

- Informed - they understand what is being shared and any consequences
- Freely given – no pressure is applied to gain consent
- Specific & Time bound – any consent must relate to the current instance of sharing and not be used for further sharing
- Evidential – you must be able to evidence that consent was given

You must retain this consent on the individuals file, as well as a record of what was shared, when and why.

Required Actions:

- Determine if the law requires the disclosure or whether you require consent of the individual
- Ensure consent, if required, is informed, and freely given
- Document the disclosure in the relevant pupil or personnel file

9. Data sharing with volunteers, work experience students, PTA, after-school clubs etc

Where you are inviting an individual into the school and they do not work for an organisation with whom you have a 'written contract,' i.e., they are independent and are not bound by an employment contract with a supplier, then you will need the equivalent of a contract with them. A non-disclosure agreement (NDA) (document E6) provides evidence that you have made the individual aware of data protection requirements when accessing personal data and evidences their agreement to conform to the standards set out in the agreement. Examples where a non-disclosure agreement is likely to be required are School Volunteers, Student Teachers, Parent-Teacher Association members, individuals who run after-school clubs etc.

Required Actions:

- Ask individuals not subject to an employment contract obliging them to comply with the school's policies to sign an NDA
- Keep a copy of the signed NDA in an appropriate file where it can be easily accessed should a query or access request be received
- Refresh non-disclosure agreements annually to ensure individuals remain aware of what they can and cannot do when accessing school data.

10. Advice and Support

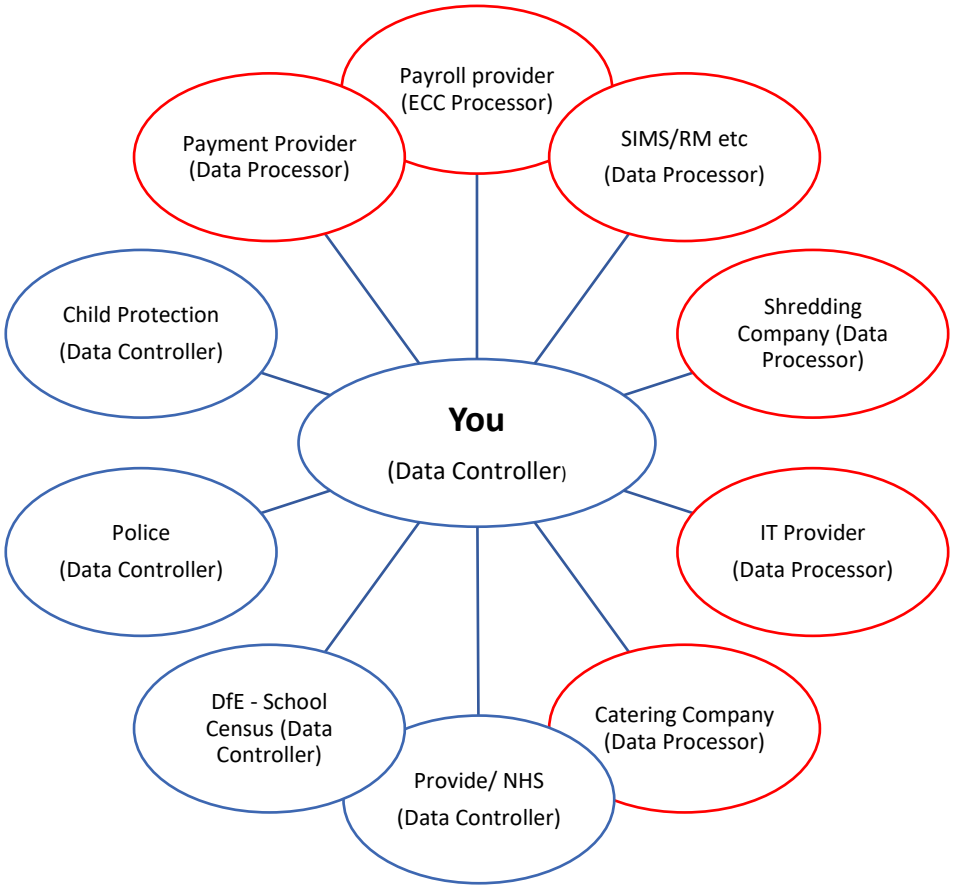
If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact the school office.

11. Breach Statement

A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

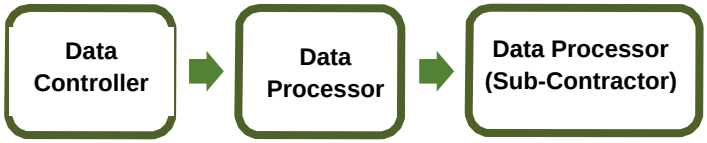
Annex A: Processors & Controllers

Diagram showing the types of Data Processor a school may work with (Green), and the types of sharing that may occur with other Data Controllers (Red).



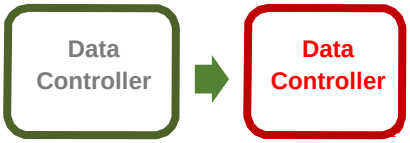
Key differences between sharing data with Processors and other Controllers

Data Controller to Data Processor



- You are always responsible for the data
- Needs a contract/ agreement
- Detailed enough to prove who is at fault for security breaches
- All subcontractors must meet the standards of the main contract Contractor

Data Controller to Data Controller



- Your responsibility for the data ends once securely provided
- You must be able to explain what allows you to share the data:
  - Understand 'legal conditions' that may support your sharing
  - Check for existing 'Information Sharing Agreements' (ISP)

Annex B: The Scope of a 'Written Contract'

These are the key commitments that GDPR (Article 28) expects Controllers to have obtained from Processors; either through a contract issued by the Controller or offered by the Processor.

The Processor will:

a) **Under Instruction**: only process personal data on documented instructions from you (the Data Controller), including about transfers of personal data to a third country (a country outside the UK) or an international organisation, unless required to do so by law. We will inform you of such a legal requirement before the transfer takes place unless the law prevents us from doing so.

b) **Confidentiality**: ensure that our employees and supplier staff authorised to process the personal data have committed themselves under contract of employment or service to maintain the confidentiality of the personal data.

c) **Security**: take all appropriate technical and organisational measures required to keep the personal data secure.

d) **Data Subject Rights**: assist you by appropriate technical and organisational measures for the fulfilment of your obligation to respond to requests for exercising data subject rights under the Data Protection Act 2018.

e) **Breach Reporting**: assist you in ensuring compliance with your obligations regarding the security of processing personal data, communicating personal data breaches and conducting Data Protection Impact Assessments, considering the information available to us.

f) **Contract End**: at your choice, delete or return all the personal data to you after the end of the provision of these services, deleting existing copies unless we are required by law to continue to store the personal data.

g) **Evidence**: make available to you all information necessary to demonstrate compliance with the personal data processing obligations laid down in this section and allow for and contribute to audits, including inspections, conducted by you or another auditor mandated by you.

h) **Instruction Concerns**: advise you immediately if any instruction received under item a) above is likely to infringe data protection law.

i) **Sub-processors**: only contract with other data processors to process personal data who comply fully with our commitment to you. Agreeing to these service terms is your general written authorisation to us that we can enter such arrangements if we inform you of any intended addition or replacement of data processors, giving you the opportunity to object to such changes. We remain liable to you for the processing of data processors engaged by us.

These commitments should be viewed as a 'minimum' requirement. They should be supplemented by further detail; the level of detail required should be dictated by the risk of the processing, i.e., processing involving large quantities of special category (sensitive) data would require more detail than processing of basic data such as name and contact details.

'Further detail' examples may include:

- A breakdown of the 'instructions' referred to in point a), i.e., the process of how the service should be undertaken.
- A description of the security measures employed by the Processor referred to in point c), d) and which should cover the process referred to in point e).
- The specific requirements of transfer or deletion referred to in point f) to avoid any confusion over responsibilities at contract end
- The specific documentation you require the Processor to maintain – point g), including potentially supplying templates such as Framework document H1.
- Specifying the process and timescales under which you would expect sub-processor notification to work under point i).