Sharing Data with Suppliers & Partners

Title	Sharing Data with Suppliers & Partners
Status	Approved
Version	V1.0
Date Approved	November 2019
Review Date	November 2020

Contents

1. Introduction

When a Data Controller uses a Data Processor to deliver services which require handling 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 (see 3.2)

The principle that the law introduces is this:

- If the Controller fails to have a compliant contract with a Processor in place then the Controller is liable for the Processor's data breach.
- 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.

2. Quick Reference Guide

- Always ensure that you have a written contract between parties, or other agreement which is legally binding on the parties
- Complete a Data Protection Impact Assessment which will guide you to consider what assurances you need from any supplier you wish to enter into a contract or agreement with
- Ensure you are clear about the roles and responsibilities of those parties to a contract or agreement. Which are Data Controllers and which are Data Processors?
- Ensure your contract stipulates that there can be no sub-contracting by a contractor without your express written consent
- Ensure that where necessary a contract or agreement is supported by an information sharing agreement or non-disclosure agreement.

3. Policy References

3.1. This procedure is a requirement of the following policies:

- Data Protection Policy

4. Procedures

3.1 Identifying Data Processors & other Controllers

4.1.1. The first step is to establish a list of all the organisations (and potentially some individuals) who you give (or allow them to obtain on your behalf) the personal data for which you are Data Controller.

4.1.2. This list should then be divided into the following (see Annexe A):

a) **Data Processors**: Organisations (or individuals) who you choose to allow access to your personal data in order to provide you a service

b) **Data Controllers**: Organisations who you are required to share your personal data with as they have a legal requirement which allows them to have it.

4.1.3. The key differences between sharing data with a Processor and another Controller are these:

a) You are always legally responsible for the actions of your Processors with personal data, unless you can evidence that they have acted outside of your 'written contract'

b) You have a responsibility to evidence that another Controller is legally entitled to your personal data and to get it to them securely, but your responsibility for it ends once it is in their custody.

4.2. Establishing & Reviewing Compliance Evidence

4.2.1. For the Data Processors on your list you will need to identify what could currently constitute a 'written contract'. 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.

4.2.2. 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.

4.2.3. For the Data Controllers on your list you will need to a) identify what allows you to share personal data with them, and b) how you will get the data to them securely. The majority of regular data sharing undertaken by schools is with other schools, a local authority, the Department for Education and NHS services. These are typically covered by existing Information Sharing Agreement/ Protocols. These should be identified and their requirements understood. They should also be reference on your data flow mapping (Document H1) to evidence how you legitimise this sharing.

4.2.4. For instances of irregular sharing, i.e. where sharing is requested without an agreement being in place, then it is important to understand that it the responsibility of the Data Controller who is asking for the data to explain why they should be legally entitled to it. 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 provides for you to share personal data with the police for this explicit purpose.

4.3. Obtaining Additional Assurances

4.3.1. After you have reviewed your existing documentation about the Data Processors' services, where you have reached the conclusion that the content does not meet the requirements explained in Annex B, you will need to obtain additional assurances.

4.3.2. There are a range of tools to help with this:

4.3.3. **Contract Schedule** (Document E1): You may decide to introduce your own contract schedule. For most Processors this would be inappropriate as their service is best managed through having consistent arrangements governing their service to all Data Controllers they work with. This document may be best used where the supplier has no documentation to

offer at all. It only addresses the information governance aspects of a service and so would not be able to be used as a standalone document; rather it will require additional documents covering other aspects of the service to form a complete contract.

4.3.4. **Supplier Policy Requirements** (Document E2): This document can be used where there is some basic documentation about the service in place but the Supplier can effectively 'sign-up' to following the school's policies as additional assurance that their processes are compliant

4.3.5. **Non-Disclosure Agreement** (Document E6): 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. Examples could be School Volunteers, Student Teachers, Parent-Teacher Association members, individuals who run after-school clubs etc. This agreement is evidence that the School has been clear about the restrictions that are in place over what an individual can do with the School's personal data.

4.3.6. **Letter to Data Processors** (Document E7): Where there is a contract in place which complies with the Data Protection 1998, but does fully cover the requirements under GDPR (Annex B), then you may wish to contact the Processor using this letter. The letter identifies the key aspects of GDPR which are not in the Data Protection Act 1998. By asking the Processor to give you specific written assurances on these points, the response will form additional assurance to the existing contract.

4.4. New Data Processors

4.4.1. 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 being able to access personal data, you will need to ensure that the 'written contract' is in place.

4.4.2. Firstly you will need to consider what assurances you are going to need from the Supplier in order to be confident that they comply with the law.

4.4.3. Typically, the high risk processing will involve processing of personal data that meets the requirement to undertake 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).

4.4.4. 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.

4.4.5. 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’ in order to satisfy the legal requirement.

4.4.6. 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.

4.5. Sharing with other Data Controllers

4.5.1. As explained above (3.2.3.) you have a duty when sharing with other Data Controllers to be able to justify why you are doing so. For sharing with the DfE, the Local Authority, other schools 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.

4.5.2. 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 Document E5). Once established, the sharing needs to be conducted in line with the provisions agreed in the Protocol. It should also be published for transparency.

4.5.3. As described above (3.2.4.) 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. These are the types of the request that would need to be referred to the Data Protection Officer as they would need specialist knowledge of the available legal provisions.

4.5.4. 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, there should be no presumption that sharing of data on request is absolutely prohibited .

5. Advice and Support

5.1. 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.

6. Breach Statement

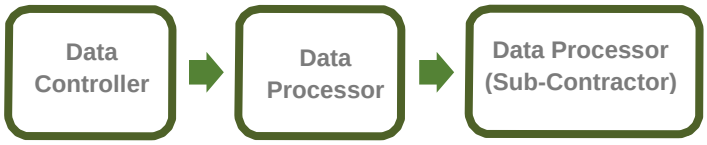
6.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

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).

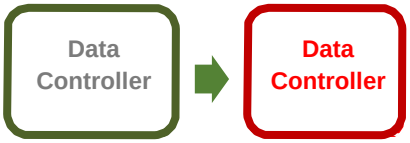
Key differences between sharing data with Processors and other Controllers

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

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 with regard to transfers of personal data to a third country (a country outside the European Economic Area) 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, insofar as this is possible, 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, taking into account 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 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, in our opinion, likely to infringe data protection law provisions.

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 into such arrangements provided that we inform you of any intended addition or replacement of data processors, thereby 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 unwanted 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).