DATA SHARING WITH THIRD PARTIES

CONTENTS

WHAT IS DATA SHARING?

Firstly, let's be clear on what exactly is meant by 'data sharing':

If you share *personal information* with *any* organisation, or third party, you are 'data sharing' for the purposes of data protection. This could include sharing information about pupils, parents, staff, governors, applicants, or visitors.

By now, you should have completed your data mapping tool and recorded all of the third party organisations with whom you share personal information. As you will see, it is useful, and often necessary, for you to transfer information about individuals as a means of meeting your obligations as a school and to providing a good education for your pupils.

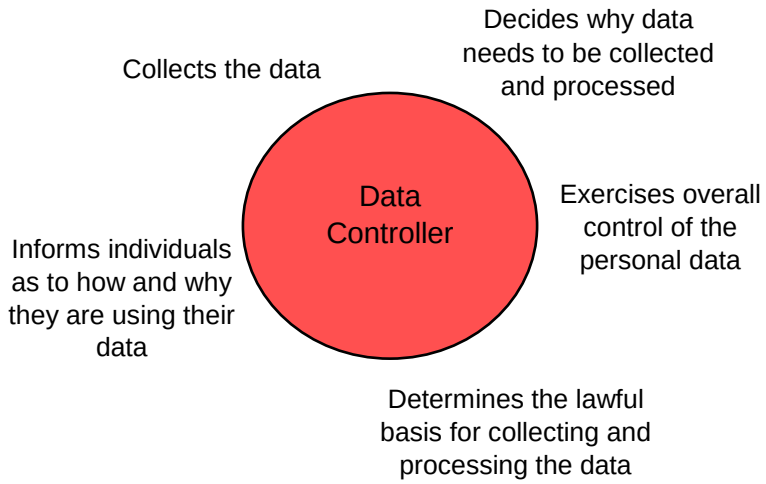
Although data sharing is, for the most part, beneficial, it is important to remember that the GDPR requires you to share information with caution. You may often share data that is highly personal in nature, and so it is crucial that the data is handled with the appropriate level of protection. Children are also regarded as vulnerable data subjects for the purposes of GDPR so their information warrants a higher level of protection. From a compliance point of view, you should also bear in mind that your school is a *data controller* which makes you ultimately accountable for the personal data it handles.

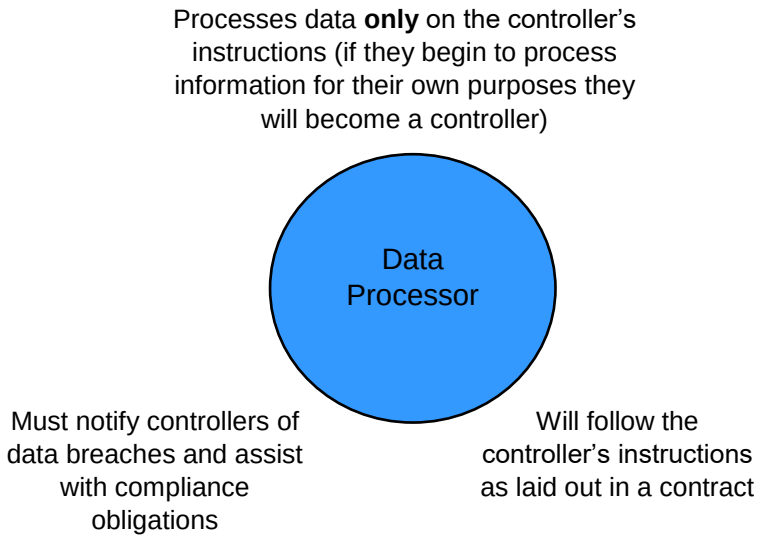
DATA PROCESSORS AND DATA CONTROLLERS

Before you share information with an organisation, you must be clear on the distinction between *data controllers* and *data processors*. This is important as this will determine what responsibilities you have. In most circumstances, your school will be acting as a *data controller*.

All organisations who process personal information must comply with data protection regulations and are therefore accountable for their processing and sharing. However, data controllers have more obligations than processors, so it is important that your school shares data securely.

Although this has been covered in previous bulletins, here is a quick summary:





To put this into perspective, the table below lays out some of the most common parties with whom schools will share information:

Organisation	**Data Controller or Data Processor?**	
Department for Education	Data Controller	
Local Authority	Data Controller	
NHS	Data Controller	
Child's New School	Data Controller	
External teacher or therapist who works independently of the school	Data Controller	
Management Information Systems (SIMS, Arbor, ISAMS)	Data Processor	
Communication Systems (Parent Pay, ParentMail, Group Call)	Data Processor	
Other kinds of information management software (CPOMS, Wonde, CSWAS, EduTrips, Evolve)	Data Processor	
Tracking Systems (O-Tracker, Tapestry, Target Tracker	Data Processor	
Educational online apps (Mathletics, Times Tables Rockstars, Spelling Shed)	Data Processor	
HR and Payroll	Data Processor	
Photography Company	Data Processor if only taking photographs on the school's instructions	May be a Data Controller if the school does not provide instructions and the photographer deals directly with parents, even though photographs are taken on school premises
External Media Organisations	Data Controller	

As you can see, there may be instances when an organisation may act as either a controller or a processor. This information should be made clear in the organisation's contract or data processing agreement. However, if it is not clear, you should seek clarification from the organisation.

The ICO defines 'processing' as the:

> *'collection, **recording**, organisation, structuring, **storage**, alteration, retrieval, consultation, use, **disclosure**, dissemination, restriction, erasure or destruction'* of data (our emphasis)

Therefore, the act of merely uploading personal data onto third party software systems, such as SIMS or CPOMS, will still count as 'data sharing'. It is therefore crucial that you take time to consider all third party systems that you use.

SHARING INFORMATION WITH DATA CONTROLLERS

Organisations, such as the ones highlighted above in red, are *data controllers*. This is because they make decisions as to what data they need to collect and how they want to use it. For example, the Department for Education will use pupil and staff data to create their own statistics and plan how they implement public policy. The Local Authority will need information from schools so they can administer and provide public services effectively. NHS Health Bodies will also use your schools data to make sure they carry out compulsory health checks.

Where a **data controller** shares information with another **data controller** (i.e. your school shares data to one of the organisations listed above) there is no requirement to have any agreement in place which formalises this data sharing process. Nevertheless, it is strongly recommended that a Data Sharing Agreement is put into place as this will lay out the obligations of each party. It also provides evidence of your school's compliance. Our blank template data sharing agreement has been attached to this Bulletin for your convenience.

NOTE: Many of you will be aware that some data controllers have not provided schools with a data sharing agreement or equivalent, even though you are required to share that information. We are not aware of anything that has been released by the Department for Education. Therefore, where you are required to share information as part of your legal obligations or public tasks, and you are struggling to obtain any kind of agreement, please do not worry.

However, if your school *makes the decision* to share information with another data controller, we would urge you to put a data sharing agreement in place as evidence of your compliance. This is particularly pertinent where you engage small businesses or sole traders, such as educational therapists or activity clubs.

SHARING INFORMATION WITH DATA PROCESSORS

Organisations such as Mathletics, Wonde and CPOMS are data processors. This is because they can only process information they receive from a data controller (i.e. your school) and act according to that controller's instructions. These instructions will be laid out in a contract or data processing agreement.

Contrary to the position on Data Controllers as described above, if you share information with any of these organisations, the GDPR makes it ***a legal requirement to have a 'contract or legal act' in place.*** This legal act must set out the nature and duration of the processing, and the responsibilities of each party. A 'legal act' can take many different names such as: *data processing agreement, data handling agreement, information processing agreement, data processing schedule* or *terms and conditions*. One of these 'legal acts' (usually a contract or terms and conditions) will normally be provided to your school when you sign up to use their services. However, where no such agreement is provided, you can use our template Data Processing Agreement, also attached to this bulletin.

The GDPR (specifically Article 28) requires a set of standard clauses to be included in that contract or legal act. *All* of these clauses must be included in order for the contract to be compliant with the GDPR. Wherever you sign up to use a third party's services, it is important that you are certain that each of these terms are included in the legal act between that processor and your school. The DPO Service can assist you in reviewing these terms.

We have attached an *Example Data Processing and Data Sharing Agreement* to this bulletin so you can see how each of these would look in action. We have also provided an explanation for each of these terms so you can understand what the obligations are for each party.

THINGS TO CONSIDER BEFORE YOU SHARE DATA

In a nutshell, whenever you plan to share information with a third party you should consider all of the steps below. In our *Record of Data Sharing with Third Parties* attached to this bulletin, we have expanded and adapted this further into a log so that you can 'tick off' each of the steps as you work your way through. We have also provided flowchart which you may want to use for a quick reference:

- Determine your purpose for sharing

  Why do you need to share information with another organisation?

  Have you already identified this on your data mapping tool?

- Ensure you have a lawful basis to justify sharing information

  You must be able to justify your data sharing under one of the following lawful bases: *legal obligation, public task, consent, contract, legitimate interest* (*vital interest* is unlikely to apply as you wouldn't be expected to form a contract if you are sharing information in an emergency situation!)

  If you need to share *special category data*, such as medical information, religion or ethnicity, you will need an additional lawful basis (see **Bulletin 4** for a full list).

  Again, this may already be identified on your data mapping tool.

- Establish what data needs to be shared

  Before you begin sharing information it is important that you know what data will be transferred to the other organisation. We always advise schools to share the *minimum* amount of data needed to fulfil the purpose.

  In a few of the contracts we have reviewed, some third party organisations have requested large amounts of data from schools without justification.

  Remember, one of the key principles of the GDPR is *data minimisation* which means that you should only process the data you need in order to fulfil your purpose.

- Consider whether a DPIA is necessary

  Some data processing activities may pose a high risk to the rights and freedoms of the data subjects. Where this is the case, you must do a DPIA *before* you begin sharing and processing the data.

  We will be providing schools with more detailed advice in relation to DPIAs in the next bulletin, so this won't be explained at length here. However, in the meantime, please revisit **Bulletin 14** or contact the DPO Service if you think a DPIA could be necessary.

  Remember, DPIAs must be completed *prior* to sharing or processing any data. This is because the purpose of a DPIA is to identify any risks that may manifest as a result of the processing, and it is an opportunity for you to ensure you are meeting all of the above criteria before you sign up.

- Obtain the relevant data sharing agreement, contract, data processing agreement, or other 'legal act'

  As already stated, many third party processors will already have a standard contract, set of terms and conditions, or data processing schedule which they will provide to you. However, where no such agreement exists you can customise our template data processing agreement and ask your suppliers to sign this instead.

  If you are provided with one from your supplier, you should check it against the template data processing agreement. If it contains all of the same clauses this will meet the requirements of the GDPR. Again, please refer it to the DPO Service if you require assistance with this as it is not an easy task.

  The same applies to other data controllers where you can use our template data sharing agreement.

  You also need to check whether information is transferred outside of the EEA. Where this is the case, it is permissible so long as the other organisation has sufficient guarantees that it is done securely.

  We should stress here that even if when your agreement meets all of the requirements of the GDPR, you must still comply with all of your other data protection obligations.

- Update your privacy notice and data mapping tool

  Your privacy notice is your way of informing all individuals of how you will use their data. This is a requirement of the GDPR as individuals have the right to be informed of how their data is used by organisations. Therefore, it should always be up to date.

  You do not have to continually provide individuals with new copies of your updated privacy notices. However, you should inform individuals if you update your privacy information. This could be done by a link sent via email or by adding a line into your school newsletter.

  Your data mapping tool must also be kept up to date as it is a legal requirement to keep a record of *all* of your school's data processing activities.

FAQS

We have been given data processing agreements which refer to 'sub-processors' or 'third party processors' – what does this mean?

Your school is the data controller and any organisation that processes data on your instructions is a data processor. However, many data processors will use the services of other data processors in order to provide their service to you.

A common example of this is Amazon Web Services who provide computing platforms such as cloud storage, servers, networks and analytics. An online educational application may well use these services in order to create their online platform and in doing so, your data will need to be shared with that sub-processor.

Another example is Wonde which schools use to integrate applications with their MIS.

It is acceptable for processors to use sub-processors, so long as they also have a data processing agreement with that sub-processor that contains all of the relevant data processing clauses referred to above.

Why do we need to check whether information is transferred outside of the European Economic Area (EEA)?

This topic won't be covered in extensive detail here. However, your school does need to check whether its information could be transferred internationally. It is easy to assume that information processed by your school is only held on site on your school network. However, the servers and storage facilities used by your suppliers can be located in other countries.

If data is not transferred outside of the EEA you won't need to take any further steps. This I because all EEA countries must all comply with the GDPR.

However, if data is transferred to non-EEA countries with weaker data protection laws and regulations, your data may not be protected to the same standards as required by the GDPR. This could mean that your school, as the data controller, is in breach of the GDPR. This will also mean that data subjects may not have the same rights over their information. For example, they may not be able to make a subject access request, or may not be aware of whom their information has been shared with or how it is being used.

Some countries have been granted an 'adequacy decision' by the EU which means you can share data with these countries as you would with any other EEA country. However, if no adequacy decision has been granted, data sharing is only permissible where prescribed safeguards have been put into place. Again, we will not explore this in extensive detail, so if

your contract states that international data transfers may be made, please contact the DPO Service who will advise you further.

If you intend to share information with US organisations, they must be certified under the EU-US Privacy Shield. We have come across a number of US companies while reviewing agreements for our schools so please be sure to check this. Where the organisation is certified, data sharing is permissible so long as all other necessary compliance measures are in place.

How will Brexit affect data sharing?

For the time being, Brexit has not changed any of your obligations in relation to GDPR or data sharing. This may change over time when deals are negotiated, however, we will clarify this as and when the time comes.

Do we need to go through all of the above if we are only sharing pupils' names?

The risks associated with sharing such a small amount of personal data are relatively low and therefore adhering to all of the above steps may seem unnecessary. That being said, you are still sharing personal data with a third party and the above rules still apply.

Do we still need a data processing agreement if we remove pupil names from the data we share?

Data protection legislation only applies to *personal data* and therefore if you do not share personal information with your suppliers you will not need to go through the steps above.

However, it is important to distinguish between *pseudonymised* data and *truly anonymous* data. Even if you use pseudonyms, nicknames or reference numbers instead of names, it may be possible to link information back to the individual it relates to, and therefore the GDPR (and all of the above steps) will still apply. For information to be truly anonymous, it must be impossible to trace it back to the individual to whom it relates.

For security reasons, it may be a good idea to use pseudonymous data. However, we would strongly advise that you consult the DPO Service before you determine that you are using anonymous data.

If we are providing the contact details of just one member of staff to a supplier, and nothing else, do we need to do a data processing agreement?

We have clarified the position on this with the ICO and they advised the following:

“There is no obligation to have a data sharing agreement with an organisation, but it is good practice in cases where a lot of data is being shared, or sensitive information. As there is not a lot of data sharing occurring in this instance, it is unlikely that a data sharing agreement would have any real effect. Just ensure the member of staff is informed that their information will be shared with this supplier.”

My local authority is responsible for handling contracts with some of our third parties. Do we need to do anything?

Where this is the case, the authority will be responsible for making the necessary checks with the supplier. However, you should still adhere to all of your other data protection obligations.