Quinton Primary School

Lawful Bases for Processing Legal Data (GDPR compliant)

In order to process personal data lawfully, you must have the individual's explicit consent, or the processing must be necessary for one of the following:

- 1) Performing a task in the public interest or in the exercise of your official authority (sometimes referred to as the 'public task' basis), for example if you are a public authority that needs to process the information to carry out your official functions
- 2) Compliance with a legal obligation
- 3) Fulfilling a contract with the individual
- 4) Protecting vital interests, i.e. to protect someone's life
- 5) Legitimate interests except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (this basis does not apply to processing carried out by public authorities, i.e. maintained schools and academies)
- 6) Additional Conditions

This information is based on the guide to the GDPR from the Information Commissioner's Office (ICO) and advice from Forbes Solicitors.

What are the lawful bases and why do they matter?

For all data processing activity you do under the GDPR, you must identify a 'lawful basis'. The lawful bases are broadly similar to the 'conditions for processing' in the Data Protection Act 1998. You should have identified your conditions for processing under the DPA, so the chances are you'll find an equivalent appropriate basis under the GDPR.

You now need to be clearer about which basis you use and when, and have a few extra steps to take with this information.

There's no hierarchy of bases, so none is 'better' than any other – the one(s) you choose in each case will depend entirely on the reason(s) you're processing the data, and your relationship with the individual it relates to.

It's important to identify your lawful basis, or bases, correctly first time, as you can't swap around later without good justification, and without having to inform everyone you've done so.

You can have multiple bases – just make sure you determine these from the outset. If you think your processing would fall under more than one basis, then document and communicate all of these, to be on the safe side.

What's important is that you have a solid justification that you are confident in and that you document your decision. If the ICO challenged you in this respect, it would be looking for evidence that you've taken data protection seriously and carefully considered your reasons for processing personal data.

What do we need to do?

Jargon buster

Personal data: any information relating to an identified, or identifiable, person.

Processing: anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Be aware that, sometimes, the basis you choose will affect the rights individuals have over their data (e.g. to have it deleted, to object to processing), which may in turn affect your ability to process it.

For example, someone can ask you to stop using their personal data if you initially used 'consent' as your lawful basis. If you determine that you need to process data to meet a legal obligation, the individual doesn't have this right.

You should have a list of all the personal data you currently hold and process.

1) Public task

This basis will cover a lot of your data processing as a school. You can rely on it if you need to process personal data in order to:

- Carry out a task in the public interest
- Exercise your official authority

You can process personal data without seeking consent if you need to in order for your school to run properly

Essentially, you can process personal data if you need to in order for your school to run properly, and to fulfil your official functions as set out in law. So, schools need to provide education to children, and if you need to process personal data about a child in order to do this, then you're allowed.

'Set out in law' doesn't mean that the law needs to specifically say "schools are required to process this type of data". It just means that your underlying task, function or power must have a clear basis in law (for example, the provision of state-funded education).

Remember: your processing needs to be a 'necessary and proportionate' way of achieving your underlying task. So you can only collect the personal data that you actually do need, and must choose the least intrusive option available to you.

Example

Schools are public authorities and so the public task basis is likely to apply to most of the processing they do, depending on the detail of their constitutions and legal powers.

For example, a school could use 'public task' for processing personal data for teaching and learning purposes as this helps you to deliver education in the public interest.

Questions to ask to see whether you can use 'public task'

- Why do we want to process this personal data?
- Is this purpose something we are required to do as a school, in order to carry out a task in the public interest? For example, does the data help us:
    - To provide education?
    - Carry out school improvement activities?

If yes, proceed to the next question. If no, this basis won't work in this case, so consider the next basis.

- Is this 'public interest task' set out in law?

If yes, proceed to the next question. (You don't need to find a specific piece of legislation, provided the overall purpose of using the information is to perform a task in the public interest and that task has a sufficiently clear basis in law, e.g. the provision of state-funded education.) If there is no basis in law to carry out the task, move on to the next basis.

- Is there another way to fulfil the task? For example, could we still do it:
    - Without processing the data at all?
    - By processing less data?
    - By collecting the data in a different, less intrusive way?

If you could make any of these changes, then this basis won't apply unless you adapt your processing. If you couldn't, and you've answered yes to all the other questions above, then you can use the public task basis.

Individual rights

If you use public task, individuals will not have the right to have their data erased, or to have it transferred to another organisation. (See the ICO's guide to the GDPR, linked to at the start of this article, for detailed information on what this means.)

2) Legal Obligation

You can use this basis if you need to process personal data to comply with a common law or statutory obligation. You should be able to identify the specific legal provision or piece of guidance that sets this out.

As above, 'set out in law' doesn't mean that the law needs to specifically say "schools/organisations are required to process this type of data". It just means that your underlying purpose must be to comply with a legal obligation.

For example, the law states that you have health and safety duties to make sure employees and visitors to your premises are safe. The law doesn't specifically say "schools must collect the names of all visitors to their premises" or "schools must show

their staff a photograph of a violent individual who is banned from the school site", but without using information in this way, you may struggle to meet your legal obligation.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

Questions to ask to see whether you can use 'legal obligation'

- Why do we want to process this personal data?
- Is this purpose something we are required to do by UK or EU law? For example, does the data enable us to:
    - Disclose employees' details to HMRC for tax purposes?
    - Keep employees safe at work?
    - Report on our gender pay gap (if required)?
    - Comply with equality legislation?
    - Report to parents?
    - Report to the Department for Education?

If yes, proceed to the next question. If no, this basis won't work in this case, so consider the next basis.

- Can we point to where these obligations are set out in law, or in an appropriate source of guidance such as a government website?

If yes, proceed to the next question. If no, you need to find the relevant legislation or guidance; if you can't find it, move on to the next basis.

- Could we still comply with the law:
    - Without processing the data at all?
    - By processing less data?
    - By collecting the data in a different, less intrusive way?

If you could make any of these changes, then this basis won't apply unless you adapt your processing. If you couldn't, then you're good to go with this basis.

Individual rights

If you use legal obligation, individuals will not have the right to have their data erased, to have it transported to another organisation, or to object to processing (again, see the ICO's guide for more information on these rights).

3) Fulfilling a contract

You can process someone's personal data if you:

- Have a contract with the person and you need to process their personal data to comply with your obligations under the contract
- Haven't yet got a contract with the person, but they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask

Example

The ICO uses the example of buying something online: when someone makes an online purchase, a data controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

In a school context, this may apply where, for example:

- *You have an employment contract with your staff, and will need to process some personal data in order to pay employees*
- *You provide CPD services to other schools or individuals, and need individuals' personal details and details of their training needs in order to do so*
- *You need to share personal data with a supplier so that they can provide the service you've contracted them for – as when you need to share staff members' bank details with your payroll provider so that they can pay staff under the terms of your contract*

Questions to ask to see if this applies

- Do we have a contract with the individual or organisation that requires the use of this personal data?

If yes, proceed to the next question. If no, this basis won't work in this case, so consider the next bases.

- Are we sure it counts as a contract? Note that your agreement doesn't have to be a formal, signed document or even written down, as long as:
    - Terms have been offered and accepted
    - Both parties intend them to be legally binding
    - There is an element of exchange

If yes, proceed to the next question. If no, move on to the next bases.

- [If the contract is with someone under 18] Are we confident the person has the necessary competence to enter into a contract?

If yes, proceed to the next question. If no, or you have doubts, consider the next bases.

- Does the data we process **only** help us deliver the contract? Or are we actually using the data for other, more general purposes?

If it only helps you fulfil the contract, proceed to the next question. If you're using it for other purposes too, you need another basis (potentially consent or legitimate interests).

- Could we still fulfil the contract:
    - Without processing the data at all?
    - By processing less data?
    - By collecting the data in a different, less intrusive way?

If you could make any of these changes, then this basis won't apply unless you adapt your processing. If you couldn't, then this one will apply.

Individual rights

If you use fulfilling a contract as your basis, individuals will not have the right to object to the data processing, or the right not to be subject to automated decision making.

4) Protecting Vital Interests

You can process personal data if it's necessary to do so to protect someone's life. This can be the individual whose data you're processing, or someone else. In a school context it will be rare that processing someone's personal data will be necessary to save the life of another, but this basis could apply if you need information about a parent in order to help a child.

You can't rely on this one if you're processing data about an individual's health and they are capable of giving consent.

So, it's likely to be used in emergencies where someone is incapable of giving consent, rather than when organising a pupil's medical care in advance, for instance.

You therefore need to anticipate, to the best of your ability, whether or not situations may arise where this basis will give you justification to process personal data, and capture these possibilities in your records and privacy notices.

Example

The ICO gives the example of an individual being admitted to the A&E department of a hospital with life-threatening injuries following a serious road accident. Disclosing the individual's medical history to the hospital is necessary in order to protect his/her vital interests.

The same principle would apply to schools where you need to share personal data with the emergency services in a situation where someone's life is at risk – if they have a sudden illness or accident, for example.

Questions to ask to see if this applies

- Do we foresee that we will ever need to process personal data to protect someone's life?

If yes, proceed to the next question. If no, you won't need this basis.

- Will these be situations where a person is incapable of consent?

If yes, you can use this basis for those situations. Make sure you document what you expect these situations to be. If no, consider the remaining bases for these situations.

5) Legitimate Interests

As a school, you can **only** use this basis where you want to process personal data that is outside the scope of your tasks as a school. For example, you might need it if your school has commercial interests that aren't related to education. (This basis is mostly for private companies, not public authorities.)

It means that you are using personal data without consent, but in a way that:

- A person would reasonably expect
- Has a minimal privacy impact
- Has a compelling justification
- Does not infringe on the interests, rights or freedoms of the individual whose personal data you're processing, particularly in the case of a child's data

The ICO has produced a lot of guidance to help you decide whether you can use this basis, as it's so broad and flexible. We recommend that you read this guidance on legitimate interests in full if you're considering it.

Questions to ask to decide whether you can use this basis

As this basis is the most flexible and broad of all of them, there are more questions to ask before you can use it – you need to ask yourself ***all of the questions below****. The ICO refers to this as a 'legitimate interests assessment'.*

Consider the personal data you are processing that you think is in your legitimate interest

- Why do we want to process the data – what are we trying to achieve, for ourselves and the individual whose data is being processed?
- Who would benefit from the processing? In what way?
- Would there be any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if we couldn't go ahead?
- Would our use of the data be unethical or unlawful, or go against industry guidelines or codes of practice, in any way?

Consider whether the processing is necessary

- Would this processing actually help us to achieve our purpose?

- Would it be a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Consider the impact of your processing and whether this overrides the interest you have identified (the 'balancing test')

- What is the nature of our relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect us to use their data in this way?
- Are we happy to explain the way we're using the data to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual? How big an impact might it have on them?
- Are we processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can we adopt any safeguards to minimise the impact?
- Can we offer an opt-out?

There's no foolproof formula for deciding whether the outcome of this test means you can use this basis – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

If this is not the right basis, and none of the other bases above apply, then you will need to use consent (see below).

Individual rights

If you use legitimate interests, individuals will not have the right to data portability.

6) Consent

We've covered consent already in our article on seeking consent for processing personal data.

You won't need to seek consent very often to process personal data - use it as a last resort

The gist is that you won't need to seek consent very often to process personal data. It's hard to get and people can withdraw it at any time, so **only use it if none of the other bases explored above apply**.

Additional conditions for special category and criminal offence data

If you're processing more sensitive personal data, you need to meet both a lawful basis outlined above and an additional condition for processing. Special category data

includes things such as ethnic origin and religious beliefs. The additional conditions are set out in the ICO's guide to the GDPR (see the sections on 'special category data' and 'criminal offence data'

However, please note that the ICO's guidance might change once the Data Protection Bill (currently going through Parliament) is finalised and enacted. We'll update this document once this happens.

What do we do once we've identified our lawful basis?

- Document your chosen lawful bases to help you demonstrate compliance – you can do this in any format you choose e.g. in a spreadsheet or in a data protection software solution you've purchased. You could also record how you decided on the relevant basis, in case you ever need to justify your decision
- Review and update your privacy notices (updated May 2018) to include information about:
    - The purposes of the processing
    - Your lawful basis/bases
    - What your 'legitimate interests' are, where you use legitimate interests as your lawful basis
- Share your updated privacy notices with individuals whose data you process, by 25 May 2018
- Where you process special category and criminal offence data, identify and document the extra conditions for processing these