



OLSJ
OUR LADY + ST JOSEPH
CATHOLIC PRIMARY SCHOOL

Subject Access Request Policy

Our Lady and St Joseph Catholic Primary School

Prepared by: P Devereux
Approved by: Governing Body
Date: March 2018
Review Date: March 2021
Checked DPO: March 2018

SUBJECT ACCESS REQUEST POLICY

‘With Christ at our centre, we love, listen and learn’

GDPR Subject Access Request Definition

The General Data Protection Regulation gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. GDPR works in two ways. Firstly it states that anyone who processes/handles personal information must comply with 6 principles, which make sure that personal information is:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up to date.
5. Held for no longer than necessary.
6. Processed in a manner that ensures appropriate security of the personal data.

Secondly, it provides a data subject (legal term for an individual) with important rights, including the right to find out what personal information is held on computer and most paper records.

A Subject Access Request

- Must be made in writing, this can be via letter, email or fax
- Must have a response issued within 30 days of a ‘valid’ request being received
- Must be made by a parent/guardian if the child is under 13 years of age
- Can be extended for up to 2 months for complex cases, the requestor must be notified of this extension

Purpose of the Policy

To ensure that:

- The correct procedures and timescales are followed when responding to a subject access request under the General Data Protection Regulation 2018

Aims

- To ensure the correct conditions are being followed for processing personal data
- To ensure correct procedures are followed
- To ensure a response is issued within correct timescale
- Commitment to operating openly and to meeting all reasonable requests for information that are not subject to specific exemption under GDPR

What do we do when we receive a SAR?

Checking of Identity

1. We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with them. However, if we have good cause to doubt your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know: a witnessed copy of your signature or proof of your address.
2. If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 16, we will need to consider whether the child can provide their consent to you acting on their behalf.
3. Should you make a data subject access request but you are not the data subject, you must stipulate the basis under the General Data Protection Regulation that you consider makes you entitled to the information.

Collation of Information

1. We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information (including 3 emails) and identify any information provided by a third party or which identifies a third party.
2. If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed we may seek legal advice on what action we should take.
3. Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual (e.g. the Authority employees), and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document. GDPR requires us to provide information not documents.

Issuing our response

1. Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at the Authority.
2. We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

Will we charge a fee?

Under the General Data Protection Regulation no fee is charged for the request of personal information.

What is the timeframe for responding to SAR's?

1. We have 30 calendar days starting from when we have received all the information necessary to identify you, to identify the information requested, to provide you with the information or to provide an explanation about why we are unable to provide the information. In many cases, it will be possible to respond in advance of the 30 calendar day target and we will aim to do so where possible.
2. It is possible for an extension of 2 months for complex cases, but you would be informed of this extension.

Not complying with a subject access request?

1. Previous Requests

If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

2. Exemptions

The Act contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Possible exemptions would be: information covered by legal professional privilege, information used for research, historical and statistical purposes, and confidential references given or received by the Authority.

What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

What if you want us to stop processing your data?

You can object to the processing of your data altogether, in relation to a particular purpose or in a particular way through a data subject notice. However, this only applies to certain processing activities and there is a

process that you must follow when making such an objection. We must then give you written notice that either we have complied with your request, intend to comply with it or state the extent to which we will comply with it and why. This information will be given to you within 21 days of receiving the data subject notice. Further information on this, can be found at www.informationcommissioner.gov.uk.

Personal Data

Personal data is information that relates to a living individual who can be identified from the information and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

1. An individual's salary or other financial information
2. Information about an individual's family life or personal circumstances, employment or personal circumstances, any opinion about an individual's state of mind
3. Sensitive personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual orientation, criminal record and membership of a trade union.

The following are examples of information, which will not normally be personal data:

1. Mere reference to a person's name, where the name is not associated with any other personal information
2. Incidental reference in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity
3. Where an individual's names appears on a document or email indicating only that it has been sent or copied to that particular individual
4. The content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.

If a document has been sent by a third party, that contains information about an individual, which relates to their personal or professional life, it is personal data. An outline of an organisation's standard procedure, relevant to an individual's complaint case will not be personal data.