Chalk Ridge Primary School

Data Subject Rights Guidance

Agreed and adopted: 8th February 2023

Reviewed 7th February 2024 Next review: 1st February 2025

This guidance is on data subject rights under the General Data Protection Regulation (GDPR) but does not cover subject access requests. There is separate guidance available to schools on subject access requests.

The data subjects rights which this guidance covers are as follows:

- **Right to rectification**:
- **Right to be forgotten/ right to erasure**
- **Right to restrict processing**
- **Right to data portability**
- **Right to object**

A. INTRODUCTION (this part applies to all of the data subject rights)

1. How must a request be made?

There is no set format for a data subject request made under the GDPR.
Requests may be made verbally or in writing. A written request can be received by fax, email, post and even social media (e.g. to the School's Facebook page or Twitter account).
A request does not have to make reference to "right to be forgotten" or any of the other requests, nor does it need to refer to an article of the GDPR. All that is required is that we can identify the individual.
Where a request is received verbally or in person we will confirm with the requester (e.g. by email) that we have understood the request, to avoid later disputes about how we have interpreted the request.
If we receive a request in this way, we will consider whether we can put on hold (delay) the period for responding to the request until we receive the requestors clarification. Where we do delay the period for responding we will inform the requestor (see section on putting on hold response period) of the reasons for putting the response on hold.
We will also keep a log of verbal requests

2. How long do we have to comply?

We must act upon the request without undue delay and at the latest **within one calendar month of receipt**.
We will calculate the time limit from the day we receive the request (whether the day is a working day or not) until the corresponding calendar date in the next month.
If the corresponding date falls on a weekend or a public holiday, we will have until the next working day to respond.

3. Can we extend the time for a response?

We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary (see below on putting on hold or extending time).

There is currently no guidance or case law to assist in deciding what is "complex". However, the ICO may well apply a restrictive approach to this.
The ICO's view is that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

4. Can we ask an individual for ID?

We are not obliged to respond to a request, unless and until we are satisfied of the requestor's identity.
If we are unsure of the identity of the requester we will seek evidence of their identity (e.g. a driving licence or passport (copies only)).
We will also usually ask for proof of address in addition if we need to send information out on paper (e.g. a recent utility bill).
We will only request information that is necessary to confirm who the requestor is. The key to this is proportionality.
We will let the requestor know without delay and within one month that we need more information from them to confirm their identity before responding to their request. We will also tell them that the timescales will begin once we receive proof of identity. The period for responding to the request begins when we receive the proof of identity (see below on putting the response period on hold).
Once we receive the proof of ID (e.g. a passport) we will record the details of the type of ID seen and the names on that ID etc and that it confirms the ID. There is no requirement for the proof of ID to then be retained.

5. Putting on hold or extending time:

Where we are

- extending the time limit where a response is complex
- or if we are putting on hold responding e.g. because we are requesting ID or clarification
- or where we are refusing to comply with a request
- or where we are requesting a fee

We will inform the individual without undue delay and within one month of receipt of the request.
We will inform the individual about:

- the reasons we are not taking action or are asking for more information;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

Where we are asking for clarification, ID or a fee we will tell the requestor that the timescales will commence when we receive the clarification, ID or fee requested.

6. What about requests for large amounts of personal data?

If the school has processed a large amount of information about an individual we can ask them for more information to clarify their request.
We will only ask for information that we reasonably need to find the personal data covered by the request.
We will let the individual know as soon as possible that we need more information from them before responding to their request.
The period for responding to the request begins when we receive the additional information.
If an individual refuses to provide any additional information, the school will still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

7. Can we refuse to comply with a request or request a fee?

We can refuse to comply with a request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
If we consider that a request is manifestly unfounded or excessive we can:

•request a "reasonable fee" to deal with the request; or
•refuse to deal with the request.
In either case we have the burden to justify our decision.
We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee we will contact the individual promptly and inform them. We do not need to comply with the request until we have received payment of the fee.
If we consider that a request may be manifestly unfounded or excessive we will promptly seek legal advice as the requirement is that we must be able to justify the decision and the test for this is expected to be difficult to meet.

8. The disclosure

If an individual makes a request electronically, we will provide the information in a commonly used electronic format, unless the individual requests otherwise.
We will provide information to the individual in a concise, transparent, intelligible and easily accessible form using clear and plain language.

B. RIGHT TO RECTIFICATION (Article 16):

Individuals have the right to have inaccurate personal data rectified.
An individual may also be able to have incomplete personal data completed. This may involve providing a supplementary statement to the incomplete data.
This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). Although we may have already taken steps to ensure that the personal data was accurate when we obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

1. Recognising requests:

A request does not need to mention the phrase 'request for rectification' or Article 16 of the GDPR to be a valid request. If the individual has challenged the accuracy of their data and has asked us to correct it or has asked that we take steps to complete data held about them that is incomplete, it will be a valid request.

2. What do we need to do?

If we receive a request, we will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary. We will take into account the arguments and evidence provided by the data subject.
What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort we will put into checking its accuracy and, if necessary, taking steps to rectify it. (e.g. we will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones).
We may also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject.

3. When is data inaccurate?

The GDPR does not give a definition of the term accuracy. However, the Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact[1].
<u>What should we do about data that records a mistake?</u>
Deciding whether personal data is inaccurate can be more difficult if the data refers to a mistake that has subsequently been resolved. The record of the mistake is, in itself, accurate and potentially should be kept. In those circumstances the fact that a mistake was made could be left and the correct information must also be included in the individual's data. It is essential that we make it clear which information is incorrect.
<u>What should we do about data that records a disputed opinion?</u>

[1] S205(1) Data Protection Act 2018

Opinions are subjective and it can therefore be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified. Where an opinion is being disputed, appending the alternative opinion with a prominent note to state whose opinion it is can be an option.

4. What should we do while we are considering the accuracy?

Under Article 18 of the GDPR an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and we are checking it. The ICO states that as a matter of good practice, we should restrict the processing of the personal data in question whilst we are verifying its accuracy, whether or not the individual has exercised their right to restriction.

5. What should we do if we are satisfied that the data is accurate?

We should let the individual know if we are satisfied that the personal data is accurate and tell them that we will not be amending the data.

We will explain our decision and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

We will place a note on our system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

6. Do we have to tell other organisations if we rectify personal data?

If we have disclosed the personal data to others, we will contact each recipient[2] and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. (we will seek legal advice if relying on disproportionate effort)

If asked to, we will also inform the individual about these recipients.

C. RIGHT TO BE FORGOTTEN/ RIGHT TO ERASURE (Article 17)

1. What is the right to erasure?

Individuals have the right to have their personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

2. What are individuals entitled to:

Individuals are entitled to obtain the erasure of personal information concerning him or her without undue delay in the following circumstances:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our only lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to erase it to comply with a legal obligation; or
- we have processed the personal data to offer information society services[3] to a child.

3. When does the right to erasure not apply?

The right to erasure <u>does not apply</u> if processing is **necessary** for one of the following reasons:

---

[2] The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

[3] Article 1(1) (b) EU Directive 2015/1535 defines information society services as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority ('public task');
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

Please note that in most cases our legal basis for processing personal data will be 'public task' or legal obligation. This means that the right to erasure will not normally apply except in limited circumstances (e.g. where the legal basis is consent (e.g. for photos)). Please also note that the right will not apply where it is necessary for us to retain the personal data (e.g. for safeguarding purposes).

Special category data

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health or social care professional e.g. a social worker).

4. Do we have to tell other organisations about the erasure of personal data?

The GDPR specifies two circumstances where we should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (e.g., on social networks, forums or websites).

If we have disclosed the personal data to others, we will contact each recipient[4] and inform them of the erasure, unless this proves impossible or involves disproportionate effort (we shall seek legal advice if relying on disproportionate effort).

If asked to, we will also inform the individuals about these recipients.

Where personal data has been made public in an online environment reasonable steps will be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data (seek legal advice if relevant).

5. How does the right to erasure apply to data collected from children?

Where we process data collected from children, we will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child.

D. RIGHT TO RESTRICTION OF PROCESSING (Article 18)

Individuals have the right to request restriction of the use of their personal data. It could be used in some situations as an alternative to asking for data to be erased and should not usually be used as a permanent measure. We may need to consider this alongside the exercise of other data subject rights. This is not an absolute right. Before we can action a request, it will need to satisfy one of the four conditions below: -

[4] See footnote 2 for definition of recipient.

1. Where the individual believes that the data is inaccurate. In this case, the requested restriction will only apply for as long as it takes to check the accuracy of the personal data.
2. Where the individual considers that the processing of the data is unlawful and they want the data to be restricted rather than erased.
3. The school no longer needs the data (e.g. it has reached the end of its retention period or could be deleted for some other reason) but the individual wants the data for the purpose of legal claims or proceedings.
4. Where the individual has objected to processing under the right to object (Article 21) and pending a decision under the right to object.

If none of the above applies, the request should be refused.
If it does apply, we will tell each individual that the restriction has been applied, unless this would be impossible or involve disproportionate effort. We will also tell the individual in advance when a restriction is going to be lifted.
If processing has been restricted under any of the above the data should only be further used in the following situations (apart from storage): -

- with the individual's consent,
- for it to be used in legal proceedings
- for the protection of the rights of another person
- for reasons of important public interest

However, we will tell any other organisation to whom we have disclosed the data that a restriction is in place, unless this would be impossible or involve disproportionate effort.

How to restrict processing

This could consist of moving the data to another system, making the data unavailable to other users, or temporarily removing published data from a website. If possible, technical measures should be taken to restrict its use. The fact that the data is restricted will be flagged up in the system.

Law Enforcement Purposes

We are aware that if the request concerns restricting information which has been used for law enforcement purposes there are some exemptions from the right to restrict processing in the DPA 2018. The DPA 2018 defines the restriction of processing as the 'marking of stored personal data with the aim of limiting its processing for the future'[5]. It is likely to apply as a temporary measure while considering the right to erasure, which also applies in a slightly different way to personal data processed for law enforcement purposes.

E. RIGHT TO DATA PORTABILITY (Article 20)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. As yet, there are no examples of how this right may affect schools. Please note that this right is not relevant to the transfer of a pupil's file from one school to another school.
In some instances, an individual has the right to receive personal data that they have provided to the school in a "structured, commonly used and machine readable format" and have the right to send these to another controller. This right will apply where the following conditions apply: -

1. The legal basis for using the personal data is consent (in respect of either personal or special category data) or
2. The legal basis for using the personal data is that it is necessary for the performance of a contract to which the individual is party or to take steps prior to entering into a contract at the request of the individual

and in the case of either point above, the data is being processed by automated means.
The right will not apply where the school's legal basis for processing the data is based on compliance with a legal obligation or performance of a task carried out in the public interest/exercise of official authority vested in the controller.

[5] S33 Data Protection Act 2018

If the individual is entitled to exercise this right, they should be able to have the data sent straight from the school to an alternative controller if they request it and if this is technically feasible.

F. RIGHT TO OBJECT (Article 21)

Individuals have the right to object to the use of their personal data where the legal basis for processing (including profiling) is: -

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or
- legitimate interests (NB: this will generally not be relevant to schools)

If an individual wants to exercise the right to object based on the above we will comply unless there are either

- compelling legitimate grounds for the processing which override the rights of the individual or
- relevant legal proceedings where access is needed to the data.

If the data has been used for direct marketing purposes, the individual has an absolute right to object. In this case, they will have been provided with the ability to opt out at any time. This also includes profiling and they will have been informed of the profiling in the privacy notice provided at the time the information was collected.

If the data has been used for scientific or historical research purposes there is a right to object unless the processing is necessary for the performance of a task carried out in the public interest.