Oakwood Infant and Nursery School

Subject Access Terms of Reference

(OAK008/05/2027)

School Mission Statement

At Oakwood Infant and Nursery School we provide a safe, healthy, happy and creative learning environment for everyone, through high expectations and mutual respect.

We are all stars, watch us shine.

Reviewed: May 2026

Approved: May 2026

To be reviewed: May 2027

About this Terms of Reference document

1. Purpose of document

2. Overview of subject access

- What is subject access?
- Does a subject access request have to be in a particular format?
- How much is the fee? What information is an individual entitled to?
- What is the time limit for responding?

Is any information exempt from subject access?

3. Taking a positive approach to subject access

4. Recognising a subject access request

- What is a subject access request?
- Formal requirements
- Requests made on behalf of others
- Requests fo r information about children
- Dealing with freedom of information requests for the requester's personal data

5. Responding to a subject access request – general considerations

- Subject access is a right of access to the personal data of a particular individual
- Responsibility of the data controller Information management systems
- Time limits Fees and cost limits
- Making reasonable adjustments for disabled people
- Confirming the requester's identity

6. Finding and retrieving the relevant information

- Extent of the duty to provide subject access
- Clarifying the request
- Finding and retrieving the relevant information
- Extent of the duty to provide subject access
- Clarifying the request
- Electronic records
- Archived information and back-up records
- Deleted information
- Information contained in emails

- Information stored on personal computer equipment
- Other records
- Amending data following receipt of subject access request
-

7. Dealing with subject access requests involving other people's information

- The basic rule Three-step approach to dealing with information about third parties
- Confidentiality
- Other relevant factors
- Responding to the request

8. Supplying information to the requester

- The information which must be supplied
- Deciding what information to supply
- The form in which the information must be supplied
- Explaining the information supplied
- Supplying information in permanent form – the application of the 'disproportionate effort' exception
- Dealing with repeated or unreasonable requests

9. Exemptions

- Exemptions and restrictions – general
- Confidential references
- Publicly available information
- Management information
- Negotiations with the requester
- Regulatory activity
- Legal advice and proceedings
- Social work records
- Health and education records
- Other exemptions

10. Special cases

- Health records
- Information about pupils held by schools
- Information about examinations

11. Enforcing the right of subject access

- Information Commissioner's enforcement powers
- Enforcement by court order
- Awards of compensation

1. Purpose of this document

The terms of reference contained in this document explain the rights that individuals have to access their personal data. It also clarifies what Oakwood Infant and Nursery School, hereafter known as 'the school' must do to comply with our duties as a data controller in this regard.

GDPR data protection principles requires the school to process personal data in accordance with the rights GDPR gives to individuals. Subject access is one of those rights. This code is intended to help provide subject access in accordance with the law and good practice. It aims to do this by explaining how the school recognise a subject access request and how it will be dealt with and responded to. It provides guidance on the limited circumstances in which personal data is exempt from subject access.

The code is a guide to our general approach, although individual cases will always be decided based on their particular circumstances.

2. Overview of subject access

What is subject access?

A Subject Access Request enables individuals to find out what personal data the school hold about them, why the school hold it, and who the school disclose it to.

Subject access is a fundamental right for individuals.

Does a SAR have to be in a particular format?

A SAR simply needs to be made in writing. Initial SARs to the school are free, but any subsequent, or persistent SARs, may require discretionary payment of a fee for dealing with the request.

What information is an individual entitled to?

Subject access is used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as an assessment of performance at work (except where this information is a trade secret).

Subject access provides a right to see the information contained in personal data, rather than a right to see copies of the documents that include that information. Although the easiest way to provide the relevant information is often to supply copies of original documents, the school is not obliged to do so.

What is the time limit for responding?

In most cases the school will respond to a subject access request promptly and in any event within 1-month of receiving it.

Is any information exempt from subject access?

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect that its disclosure is likely to have. There are also some restrictions on disclosing information in response to a SAR – where this would involve disclosing information about another individual, for example.

3. Approach to subject access

The school takes a positive approach to subject access, and has the following indicators of good practice:

Training

SAR training is given to all staff as part of induction and logged on a database monitored by training staff. Refresher training is delivered either as part of generic data protection training or on a more specialised basis dependant on job role.

Guidance

Dedicated data protection information is available for staff.

Request handling staff

There is a central team responsible for responding to requests, and there is more than one member of staff aware of how to process a SAR so there is resilience against absence.

Arrangements are in place for responses to SARs to be reviewed by a senior manager in the event that a requester is dissatisfied with the initial response.

Data protection experts

Oakwood Infant and Nursery has engaged an external 3rd party organisation of data protection experts or 'Information Champions' to provide data protection expertise.

Monitoring compliance

Compliance with SARs is monitored and discussed at Information Governance Steering Group meetings, and management information is kept showing the number of SARs received. Details of any requests which have not been actioned within the statutory time limit are escalated to the senior leadership team, so that any breach is addressed at a senior level.

Requests made on behalf of others

GDPR legislation does not prevent an individual making a subject access request via a third party. It could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, the school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Requests for information about children

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, e.g., to a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of the children these rights are likely to be exercised by those with parental responsibility for them.

When considering such requests, the following, among other things should be taken into account:

- The nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information

The school may receive a SAR in the form of a freedom of information request because it is deemed to be a public authority for the purposes of the FOIA or the Environmental Information Regulations 2004 (EIR). Therefore, the school will deal with the request appropriately, which will depend upon whether it relates exclusively to the requester's own personal data or whether it relates to other information as well.

If it is clear that the requester is merely requesting their own personal data, but they have cited FOIA, the school will do the following:

- Deal with the request as a SAR in the normal way. The requester does not need to make a new request.
- The school may need to ask for payment of any necessary fee
- Ask the individual to verify their identity
- The school will clarify within 20 working days (the time limit for responding to FOI requests) that the request is being dealt with as a SAR under GDPR, and that the 1-month time limit for responding applies.

NB. The school is a public authority, therefore requested personal data is, in fact, exempt from disclosure under FOIA or the EIR. Strictly speaking, the school should issue a formal refusal notice to this effect. In practice, however, we would not do so where the request is being dealt with as a SAR.

If the request relates to information which cannot be requested by means of a SAR (e.g., it includes a request for non-personal information) then the school will treat this as two requests: one for the requester's personal data made under GDPR; and another for the remaining, nonpersonal information made under FOIA. If any of the non-personal information is environmental, the school should consider this as a request made under the EIR.

It is important that we consider the requested information under the right legislation. This is because the test for disclosure under FOIA is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA to the world at large, this could lead to a breach of the data protection principles.

4. Recognising a subject access request

What is a subject access request?

A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for based on section 7 of the Data Protection Act 1998 (DPA). There are however changes, GDPR retains all the existing rights but also enhances them.

Changes to be aware of are:

- There is no fee for processing a SAR unless:
    - additional copies are requested where an administrative fee can be charged; or
    - a request is "manifestly unfounded or excessive" and for which a reasonable charge could be applied

- SARs could be refused on grounds of "manifestly unfounded or excessive" requests. Under the current code of practice issued by the ICO it is made clear that every effort should be made to comply with a request as far as reasonably practicable.
- Electronic Requests - Where a SAR is made electronically, the information should be provided in a commonly-used electronic form unless requested otherwise
- The time limit to respond has been reduced to "within 1-months" and without unreasonable delay. This can be extended for a further 2 months where requests are particularly complex, and the data subject has been notified of the extension

The request does not have to be in any particular form. Nor does it have to include the words 'subject access' or make any reference to GDPR. A request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act (FOIA).

Formal requirements

A SAR must be made in writing. Standard forms can make it easier to recognise a subject access request and make it easier for the individual to include all the details the school might need to locate the information they want. However, there is no legally prescribed request form. Although The school may invite individuals to use a request form, it should made clear that this is not compulsory, and the school will not use this as a way of extending the 1-month time limit for responding.

A request sent by email or fax is as valid as one sent in hard copy. SARs might also be received via the school Facebook page, other social media sites to which the school may subscribe, and possibly via third party websites.

The school, prefers that SAR requests are sent by email to admin@oakwood.essex.sch.uk but will still respond to SARs which are sent by other means.

The following points will be used when considering validity:

- The school need not respond to a request made verbally but, depending on the circumstances, it might do so (as long as the school is satisfied about the person's identity), and will at least explain to the individual how to make a valid request, rather than ignoring them.
- If a request does not mention GDPR specifically or even say that it is a subject access request, it is nevertheless valid and will be treated as such if it is clear that the individual is asking for their own personal data.
- The requester does not have to tell the school their reason for making the request or what they intend to do with the information requested (although it may help to find the relevant information if they do explain the purpose of the request).
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests

5. Responding to a subject access request – general considerations

Subject access is a right of access to the personal data of a particular individual

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Before The school can respond to a subject access request (SAR), we need to be able to decide whether information we hold is personal data and, if so, whose personal data it is.

GDPR legislation provides that, for information to be personal data, it must relate to a living individual and allow that individual to be identified from that information (either on its own or in conjunction with other information likely to come into the organisation's possession). The context in which information is held, and the way it is used, can have a bearing on whether it relates to an individual and therefore on whether it is the individual's personal data.

In most cases, it will be obvious whether the information being requested is personal data, but the ICO have produced separate guidance to help decide in cases where it is unclear.

The same information may be the personal data of two (or more) individuals. Additional rules apply where responding to a SAR may involve providing information that relates both to the individual making the request and to another individual.

Responsibility of the data controller

If the school determine the purpose for which and the manner in which the personal data in question is processed, then we are/is the data controller in relation to that personal data and will be responsible for responding to the SAR. GDPR does not allow any extension to the 1-month time limit in cases where we have to rely on a data processor to provide the information.

The duty to comply with a SAR promptly clearly implies an obligation to act without unreasonable delay but, equally clearly, it does not oblige the school to prioritise compliance over everything else. The 1-month long stop period is generally accepted as striking the right balance in most cases between the rights of individuals to prompt access to their personal data and the need to accommodate the resource constraints of organisations to whom SARs are made.

Provided that the school deal with the request in the normal course of business, without unreasonable delay, and within the 1-month period, we are likely to comply with the duty to comply promptly.

Confirming the requester's identity

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, the school need to be satisfied we know the identity of the requester. We can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on their behalf).

The key point is that the school must be reasonable about information we ask for. We should not request lots more information if the identity of the person making the request is obvious to the school. This is particularly the case, e.g., when the school have an ongoing relationship with the individual

The school will respond effectively to SARs, and has the following indicators of good practice:

- Managing expectations:
    - Guidance is available on the school's website which provides details of the 1-month time limit for responding to a SA, and that each request will be acknowledged with a letter or email informing the requester of the date by which a response must be provided. If there is a delay in dealing with the request for any reason, the requester will be contacted to explain the reason and the expected date for receipt of the response.
- The response to a SAR includes an explanation of the searches which have been made to deal with the request and the information revealed by those searches. This will allow the requester to understand whether they have received all the information to which they are entitled.

Logs and checklists

The receipt of SARs will be logged, and the log is updated to monitor progress as the SAR is processed within the school organisation. The log includes copies of information supplied in response to the SAR, together with copies of any material withheld and an explanation of the reasons for this.

A standard checklist is used to ensure consistency in identity verification procedures and any fee collection, and to ensure that the necessary information is obtained from relevant departments across the organisation. The checklist forms a coversheet which is put on file for each SAR that is received.

Where a data processor is involved, the school will ensure that the data processor is aware of its obligations with regard to subject access prior to appointment, and a clause specifying the organisation's requirements in terms of SAR handling should be included in the written contract.

6. Finding and retrieving the relevant information.

Extent of the duty to provide subject access

In some cases, dealing with a subject access request (SAR) may be a challenging task. This might be because of the nature of the request, because of the amount of personal data involved, or because of the way in which certain information is held. In this chapter, we consider the extent of the right of subject access in relation to categories of information which, depending on the circumstances, may be difficult to access. We also explain what the school may require from the requester, in terms of additional information to help the school find the data to which their request relates.

It should be noted at the outset that GDPR does not permit the school to exclude information from a response to a SAR merely because that information is difficult to access. Although the so-called 'disproportionate effort' exception applies to supplying the information to the requester in permanent form, it does not apply to finding and retrieving that information in the first place. The school must make extensive efforts to locate personal data that is relevant to a SAR. Having made those efforts, however, the school are not obliged to leave no stone unturned in the search for relevant information.

Clarifying the request

Before responding to a SAR, the school may ask the requester for information that we reasonably need to find the personal data covered by the request. We need not comply with the SAR until we

have received this information. However, even if the relevant information is difficult to find and retrieve, it is not acceptable for the school to delay responding to a SAR unless we can reasonably require more information to help find the data in question.

The school cannot require the requester to narrow the scope of their request, but merely to provide additional details which will help us locate the requested information. So, if a requester asks for 'all the information the school hold' about them, they are entitled to do that. The school may ask them to provide information about the context in which information about them may have been processed, and about the likely dates when processing occurred, if this will help us to deal with the request.

The school should not ignore a request simply because more information is needed from the requester. We should not delay in asking for this but should ensure the requester knows the school need more information and should tell them what details are needed. Provided we have done so, the 1-month period for responding to the request does not begin to run until we have received any appropriate fee and any additional information that is necessary.

The type of information that it might be reasonable for the school to ask for includes, where personal data is held in electronic form, information as to the type of electronic data being sought (application form, letter, email etc) and the approximate date of the creation of the data. This may assist us in identifying whether the information sought is likely to have been archived (either printed off and held in a manual data archive or removed from 'live' electronic data systems and held in an electronic archive) or deleted.

Electronic records

In most cases, information stored in electronic form can easily be found and retrieved. However, given that it is extremely difficult to truly erase all electronic records, it is arguable that a requester might be entitled to request access to personal data that the school do not have ready access to –we still hold the data, and, with time and varying degrees of technical expertise, we could retrieve it.

The school are likely to have removed information from 'live' systems in a number of different ways. The information may have been:

- 'archived' to storage;
- copied to back-up files; or
- 'deleted'.

Archived information and back-up records

Generally speaking, information is archived because, although we wish to remove it from live systems we may have decided to retain a copy in case it is needed in the future.

The suppliers of IT services to the school have procedures in place to find and retrieve personal data that has been electronically archived or backed-up. The process of accessing electronically archived or backed-up data may be more complicated than the process of accessing 'live' data. However, as we may have decided to retain copies of the data for future reference, the school will be able to find the data (possibly with the aid of location information from the requester), and the school will therefore be required to provide such information in response to a SAR.

Electronic archive and back-up systems may not use as sophisticated search mechanisms as 'live' systems, and the school may ask a requester to provide us with enough contextual information

about their request to enable us to make a targeted search for the relevant information. The ability of the requester to provide such information may have a significant impact upon whether we can find the information in question. Nevertheless, to the extent that search mechanisms allow us to find archived or backed-up data for our own purposes, the school will use the same effort to find information in order to respond to a SAR.

If a request relates specifically to back-up copies of information held on the school 'live' systems, it is reasonable to consider whether there is any evidence that the back-up data differs materially from that which is held on the 'live' systems and which has been supplied to the requester. Where there is no evidence that there is any material difference, the Information Commissioner would not seek to enforce the right of subject access in relation to the back-up records.

Deleted information

Information is 'deleted' when the school attempt to permanently discard it and we have no intention of ever attempting to access it again. It is the Information Commissioner's view that, if the school delete personal data held in electronic form by removing it (as far as possible) from our computer systems, the fact that expensive technical expertise might enable the deleted information to be recreated does not mean that we must go to such efforts to respond to a SAR. The Commissioner would not seek to take enforcement action against an organisation which has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form. The Commissioner does not require organisations to expend time and effort reconstituting information that they have deleted as part of their general records management arrangements.

In coming to this view, the Information Commissioner has taken account of the fact that the purpose of subject access is to enable individuals to find out what information is held about them, to check the accuracy of that information and ensure that it is up to date, and where information is incorrect, to request correction of the information or compensation where inaccuracies have caused them damage or distress. However, where the school have deleted the information, and can no longer use it to make decisions affecting the individual and any inaccuracies in the information can have no effect as the information will no longer be accessed by the school or by anyone else.

Information contained in emails

The contents of emails stored on the school computer systems are, of course, a form of electronic record to which the general principles set out above apply. For the avoidance of doubt, the contents of an email should not be regarded as deleted merely because the email in question has been moved to a user's 'Deleted items' folder.

It may be particularly difficult to find information to which a SAR relates if that information is contained in emails which have been archived and removed from the school 'live' systems. Nevertheless, the right of subject access is not limited to the personal data to which it would be 'reasonable' for us to provide access. Subject to certain exemptions, the school must provide subject access to all personal data which we hold, regardless of how difficult it is to find. The school may, of course, ask the requester to provide us with contextual information to help us find the personal data they have requested.

Usually, once the relevant emails have been found, the cost of supplying a copy of the personal data contained within them is unlikely to be prohibitive. The school cannot refuse to comply with a SAR on the basis that it would involve disproportionate effort simply because it would be costly and time consuming to find the requested personal data held in archived emails.

Information stored on personal computer equipment

The school are only obliged to provide personal data in response to a SAR if we are a data controller in respect of that data. In the large majority of cases, therefore, the school do not have to supply personal data if it is stored on someone else's computer systems rather than the school's own (the obvious exception being where that person is a data processor. However, if the requester's personal data is stored on equipment belonging to the school staff (such as smartphones or home computers) or in private email accounts, and the school staff hold personal data on their own devices, they may be processing that data on The school behalf, in which case it would be within the scope of a SAR which is made to the school.

The school have a policy restricting the circumstances in which staff may hold information about pupils or other employees on their own devices or in private email accounts.

Other records

The school may hold information about the requester otherwise than in electronic form (e.g. in paper files or on microfiche records) and will need to decide whether that information is covered by the right of subject access. The school will need to make a similar decision if electronic records have been removed from the school live systems and archived in non-electronic form.

Whether the information contained in such hard copy records is personal data accessible via the right of subject access will depend primarily on whether the non-electronic records are held in a 'relevant filing system' and on whether sufficient contextual information has been provided by the requester to enable the school to find the information requested.

Amending data following receipt of a SAR

GDPR legislation specifies that a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while we are dealing with the request. So, it would be reasonable for the school to supply information we hold when we send out a response, even if this is different to that held when the school received the request.

However, it is not acceptable to amend or delete the data if the school would not otherwise have done so. For organisations subject to the Freedom of Information Act (FOIA), it is an offence to make such an amendment with the intention of preventing its disclosure.

A requester can be asked to give details of the specific information which is requested. By narrowing the scope of the request (where possible) it is often possible to avoid making unnecessary searches or sending the requester large amounts of information that they do not want or expect.

As part of the SAR logging process, a check must be made to establish whether the request is sufficiently clear. If it is not immediately obvious what the request relates to, or where the personal information the requestor requires is located, the requestor should be contacted to discuss the matter. A check should also be made to ensure that the address to which the response is to be sent is known.

Asset registers

An information asset register is in place which documents where and how personal data is stored within the organisation; this helps speed up the process of locating the information required to respond to SARs

Retention and deletion policies

There are documented retention and deletion policies relating to the personal information the organisation holds. Different retention periods apply to different classes of information, depending upon the purpose for which it is held.

Monitoring

If the organisation receives a significant volume of SARs, the team which deals with them holds weekly meetings to discuss SAR progress and to investigate any cases which appear to be experiencing delay.

7. Dealing with subject access requests involving other people's information

The basic rule

Responding to a subject access request (SAR) may involve providing information that relates both to the requester and to another individual.

The GDPR legislation states that the school do not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

So, although we may sometimes be able to disclose information relating to a third party, we need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway.

The school should make decisions about disclosing third party information on a case by case basis. and must not apply a blanket policy of withholding such information.

For the avoidance of doubt we cannot refuse to provide subject access to personal data about an individual simply because we obtained that data from a third party. The rules about third party data apply only to personal data which includes information about the individual who is the subject of the request and information about someone else.

Three step approach to dealing with information about third parties

To help the school decide whether to disclose information relating to a third-party individual, it helps to follow the three-step process described below.

Step 1 – Does the request require the disclosure of information which identifies a third-party individual?

We should consider whether it is possible to comply with the request without revealing information which relates to and identifies a third-party individual. In doing so, we should not only take into account the information we are disclosing, but also any information which we reasonably believe the

person making the request may have, or may get hold of, that would identify the third-party individual.

As our obligation is to provide information rather than documents, we may delete names or edit documents if the third-party information does not form part of the requested information.

However, if it is not possible to separate the third-party information from that requested and still comply with the request, we need to take account of the following considerations.

Step 2 – Has the third-party individual consented?

In practice, the clearest basis for justifying the disclosure of third party information in response to a SAR is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a SAR.

However, there is no obligation to try to get consent and there will be some circumstances where it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. Indeed, it may not always be appropriate to try to get consent (for instance, if to do so would inevitably involve a disclosure of personal data about the requester to the third party).

Step 3 – Would it be reasonable in all the circumstances to disclose without consent?

In practice, it may sometimes be difficult to get third party consent, e.g. the third party may refuse consent, or may be difficult to find. If this is the case, we must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway.

GDPR provides a non-exhaustive list of factors to be taken into account when making this decision.

These include:

- any duty of confidentiality owed to the third-party individual;
- any steps the school have taken to try to get the consent of the third-party individual;
- whether the third-party individual is capable of giving consent; and
- any express refusal of consent by the third-party individual.

Confidentiality

Confidentiality is one of the factors which the school must take into account when deciding whether we should disclose information about a third party without their consent. A duty of confidence arises where information which is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to the school with the expectation that it will remain confidential. This expectation might result from the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and patient)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

However, we should not always assume confidentiality. For example, a duty of confidence does not arise merely because a letter is marked 'confidential', (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so it does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.

In most cases where a duty of confidence does exist, it will usually be reasonable to withhold third party information unless the school have the consent of the third-party individual to disclose it.

Other relevant factors

In addition to the factors listed in GDPR, the following points are also likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

- Information generally known by the individual making the request.

If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely to be reasonable for the school to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual

- Circumstances relating to the individual making the request.

The importance of the information to the requester may also be a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending upon the significance of the information to the requester, it may be appropriate to disclose it even where consent has been withheld by the third party.

- There are special rules governing subject access to health, educational and social work records.

In practice, these rules are such that relevant information about health, education or social work professionals (acting in their professional capacities) should usually be disclosed in response to a SAR.

Responding to the request

Whether we decide to disclose information about a third party in response to a SAR or to withhold it, we will need to respond to the requester. If the third party has given their consent to disclosure of information about them, or if the school are satisfied that it is reasonable in all the circumstances to disclose it without consent, the school should provide the information in the same way as any other information provided in response to the SAR.

If the school have not got the consent of the third party, and we are not satisfied that it would be reasonable in all the circumstances to disclose the third-party information, then we should withhold it. However, we are still obliged to communicate as much of the information requested as we can without disclosing the identity of the third-party individual. Depending upon the circumstances, it may be possible to provide some information, having edited or 'redacted' it to remove information which would identify the third-party individual.

The school must be able to justify the decision to disclose or withhold information about a third party, and so it is good practice to keep a record of what we decide, and why. For example, it would be sensible to note why we l chose not to try to get consent or why it was not appropriate to try to do so in the circumstances.

8. Supplying information to the requester

The information which must be supplied

The focus of a subject access request (SAR) is usually on the supply of a copy of the requester's personal data. Subject access entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- told whether any personal data is being processed – so, if the school hold no personal data about the requester, we must still respond to let them know this;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- given details of the source of the data (where this is available).

This information might be contained in the copy of the personal data we supply. To the extent it is not, however, we must remember to supply this information in addition to a copy of the personal data itself when responding to a SAR.

The requester may also ask for an explanation of the reasoning behind any automated decisions taken about him or her, such as an assessment of performance at work (except where this information is a trade secret). The school only need provide this additional information if it has been specifically requested. Before supplying any information in response to a SAR, we should check that we have the requester's correct postal and/or email address. If we are supplying information by fax (and we recommend that we do so only if the requester specifically asks us to), then we must ensure that we are sending it to the correct fax number.

Deciding what information to supply

Documents or files may contain a mixture of information that is the requester's personal data, personal data about other people and information that is not personal data at all. This means that sometimes the school will need to consider each document within a file separately, and even the content of a particular document, to assess the content of the information they contain.

It may be easier (and will be more helpful) to give a requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it is their personal data – this approach is likely to be appropriate where none of the information is particularly sensitive or contentious.

The form in which the information must be supplied

Once we have located and retrieved the personal data which is relevant to the request, the school must communicate it to the requester in intelligible form. In most cases, this information must be communicated to the requester by supplying him or her with a copy of it 'in permanent form'. The school may comply with this requirement by supplying the requester with a photocopy or print-out of the relevant information.

If a SAR has been made electronically, it is likely that the requester will be content with – and may even prefer – the response to be sent electronically too. If they agree to information being supplied in electronic form, then the school will comply with GDPR legislation by doing so.

Subject access provides a right to see the information contained in personal data, rather than a right to see copies of the documents that include that information. The school may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents which contain the personal data), or by providing a print-out of the relevant information from our computer systems. Although the easiest way to provide the relevant information is often to supply copies of original documents, we are not obliged to do so.

Explaining the information supplied

GDPR legislation requires that the information the school supply to the individual is in 'intelligible form'. At its most basic, this means that the information we provide should be capable of being understood by the average person. However, GDPR does not require us to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

There are two situations in which the obligation to supply the requester with a copy of the relevant information 'in permanent form' does not apply. The first is where the requester agrees to another arrangement, and the second is where the supply of such a copy is not possible or would involve disproportionate effort.

GDPR does not define 'disproportionate effort' but it is clear that there is some (albeit limited) scope for assessing whether complying with a request would result in so much work or expense as to outweigh the requester's right of access to their personal data. However, it should be noted that this qualification to the right of subject access only applies in respect of 'supplying' a copy of the relevant information in permanent form. So, the school cannot refuse to deal with a SAR just because we think that locating the information in the first place would involve disproportionate effort.

The school will rely on the disproportionate effort exception only in the most exceptional of cases. The right of subject access is central to data protection law, and even if we can show that supplying a copy of information in permanent form would involve disproportionate effort, the school must still comply with the request in some other way.

In addition, even if we do not have to supply a copy of the information in permanent form, the requester still has the right:

- to be informed whether the school are processing their personal data; and
    - if so, to be given a description of:
        - the personal data in question;
        - the purpose of the processing;
        - and the recipients or classes of recipients; and
        - to be given information about the source of the personal data.

Dealing with repeated or unreasonable requests

GDPR does not limit the number of SARs an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says that the school are not obliged to comply with an identical or similar request to one which the school have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

GDPR gives the school some help in deciding whether requests are made at reasonable intervals. It says that the school should consider the following.

- The nature of the data – this could include considering whether it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause detriment to the requester.
- How often the data is altered – if information is unlikely to have changed between requests, the school may decide that they are not obliged to respond to the same request twice.

If, for these reasons, if the school decides that they are not obliged to provide the information requested, the school will explain this to the requester. They may not realise, for example, that records have not changed since their last request.

The school has effective mechanisms in place for supplying information to requesters, and has the following indicators of good practice:

Online and electronic formats

- If requested, personal information is supplied in a machine-readable and re-useable format.
- Onsite viewing facilities There are procedures in place for requester to view the requested information on the premises if it is voluminous or may require further support and/or explanation.
- Copy differentiation - SAR response hard copies are stamped 'data subject copy' prior to release. This may assist in identifying the source of any further disclosure of the information, should the need arise.

9. Exemptions

Exemptions and restrictions – general

GDPR legislation recognises that there are some circumstances in which the school might have a legitimate reason for not complying with a subject access request (SAR). It provides a number of exemptions from the duty to provide subject access. Where an exemption applies to the facts of a particular request, we may refuse to provide all or some of the information requested, depending upon the circumstances. It is a matter for the school to decide whether or not to use an exemption from subject access – GDPR does not oblige us to do so, and it is therefore open to us to comply with a SAR regardless of the availability of an exemption.

Certain restrictions (similar to exemptions) are also built into GDPR's subject access provisions. For example, there are restrictions on the disclosure of personal data about more than one individual in response to a SAR.

The school should look at each exemption carefully to see what effect it has in respect of a particular SAR. Some exemptions apply because of the nature of the personal data in question, e.g. information contained in a confidential reference. Others apply because disclosure of the information would be likely to prejudice a particular function of the organisation to which the request is made. GDPR does not explain what is meant by 'likely to prejudice'. However, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned.

If challenged, the school must be prepared to defend any decision to apply an exemption, to the Information Commissioner's Office or a court. It is therefore good practice to ensure that any such decisions are taken at an appropriately senior level we document the reasons for the decision.

Confidential references

From time to time the school may give or receive references about an individual, e.g. in connection with their employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean that the personal data included in the reference is exempt from subject access. GDPR legislation makes a distinction between references the school give and references the school receive:

- References the school give are exempt from subject access if they are given in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.
- There is no such exemption for references the school receive from a third party. If we receive a SAR relating to such a reference, we must apply the usual principles about subject access to decide whether to provide some or all the information contained in the reference.

It may be difficult to disclose the entirety of a reference to the individual it relates to without disclosing some personal data about the author of the reference – most obviously, their identity. If the reference was not provided in confidence, this should not prevent disclosure. However, where a question of confidentiality arises, we should contact the author to find out whether they object to its disclosure, and (if so) why.

Even if the provider of a reference objects to its disclosure in response to a SAR, the school will need to supply the personal data it contains to the requester if it is reasonable to do so in all the circumstances. The school will therefore need to weigh the referee's interest in having their comments treated confidentially against the requester's interest in seeing what has been said about them. Relevant considerations are likely to include:

- any express assurance of confidentiality given to the referee;
- any reasons the referee gives for withholding consent;
- the likely impact of the reference for the requester;
- the requester's interest in being able to satisfy him or herself that the reference is truthful and accurate; and
- any risk disclosure may pose to the referee.

Publicly available information

Where an organisation is obliged by or under an enactment to make information available to the public, personal data that is included in that information is exempt from the right of subject access.

The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about the individuals, the additional data is not exempt from the right of subject access even if the organisation publishes that data.

Management information

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the activity of the organisation.

Regulatory activity

Some organisations may use an exemption from subject access if they perform regulatory activities. The exemption is not available to all organisations, but only to those that have regulatory functions concerning the protection of the public or charities, or fair competition in business. Organisations which do have such functions may only apply the exemption to personal data processed for these core regulatory activities, and then only to the extent that granting subject access to the information concerned would be likely to prejudice the proper discharge of those functions.

Legal advice and proceedings

Personal data is also exempt from the right of subject access if it consists of information for which legal professional privilege (or its Scottish equivalent, 'confidentiality in communications') could be claimed in legal proceedings.

The English law concept of legal professional privilege encompasses both 'legal advice' privilege and 'litigation' privilege. In broad terms, the former applies only to confidential communications between client and professional legal adviser, and the latter applies to confidential communications between client, professional legal adviser or a third party, but only where litigation is contemplated or in progress.

The Scottish law concept of confidentiality of communications provides protection both for communications relating to the obtaining or providing of legal advice and for communications made in connection with legal proceedings. Information that comprises confidential communications made between client and professional legal adviser may be withheld under the legal privilege exemption in the same way that information attracting English law 'legal advice' privilege may be withheld. Similarly, the Scottish law doctrine that a litigant is not required to disclose material which he has brought into existence for preparing his case protects information that, under English law, would enjoy 'litigation' privilege.

Where legal professional privilege cannot be claimed, however, the school may not refuse to supply information in response to a SAR simply because the information is requested in connection with actual or potential legal proceedings. GDPR contains no exemption for such information and, indeed, it provides that the right of subject access overrides any other legal rule which limits disclosure. In addition, there is nothing in the Act which limits the purposes for which a SAR may be made, or which requires the requester to tell the school what they want the information for.

It has been suggested that case law provides authority for organisations to refuse to comply with a SAR where the requester is contemplating or has already begun legal proceedings. Whilst the Information Commissioner does not accept this view, he recognises that the courts have discretion as to whether or not to order compliance with a SAR and that, where a court believes that the disclosure of information in connection with legal proceedings should, more appropriately, be determined by the Civil Procedure Rules (the courts' rules on disclosure), it may refuse to order personal data to be disclosed.

Nevertheless, simply because a court may choose not to order the disclosure of an individual's personal data does not mean that, in the absence of a relevant exemption, GDPR does not require the school to do so. It simply means that the individual may not be able to enlist the support of the court to enforce his right.

Social work records

There are special rules which apply where providing subject access to information about social services and related activities would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the requester or any other person.

These rules are set out in the Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415), and their effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would be likely to cause such harm.

There is a further exemption from subject access to social work records which applies in cases where a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has indicated that they do not want it to be disclosed to that third party.

Health and education records

The exemptions which may apply when a SAR relates to personal data included in health and education records are explained in chapter 10 of the code.

Other exemptions

The exemptions mentioned in this chapter are the ones which are most likely to apply in practice. However, GDPR contains a number of additional exemptions which may be relevant when dealing with a SAR.

An organisation which makes appropriate use of the exemptions in GDPR might have the following indicators of good practice:

Withholding or redacting information:

- If information is withheld in reliance on an exemption, the response explains, to the extent it can do so, the fact that information has been withheld and the reasons why. The explanation is given in plain English and does more than simplify specify that a particular exemption applies.
- Information to be redacted is approved before source material is copied in a redacted form and it is then subject to at least one quality review by a manager to confirm that all data has been excluded appropriately. A copy of the disclosure bundle showing the redactions and the reasons behind them is retained for reference.
- Once approved, redaction is either carried out manually using black marker which is then photocopied, or electronically using Adobe Acrobat or bespoke redaction software.
- Ensuring consistency Advice on applying the exemptions most likely to be relevant to the organisation's activities is included in SAR guidance for staff.
- Quality assessments are carried out to ensure consistency of application of exemptions.

10. Special cases

Health records

What is a health record?

For the purposes of the GDPR legislation, a 'health record' is a record which:

- consists of information relating to the physical or mental health or condition of an individual; and
- has been made by or on behalf of a health professional in connection with the care of that individual.

'Health professionals' include registered medical practitioners, dentists and nurses and clinical psychologists. GDPR provides a full list of the types of professional which fall within the definition.

Information which forms part of a health record about a living individual is the personal data of the individual it relates to, irrespective of the form in which it is held. This means that a subject access request (SAR) can be made for health records which are kept in manual form, e.g. on paper or in GP's medical notes wallets, as well as for health records which are kept electronically.

Information about pupils held by schools

A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by the school. If the school is in England, Wales or Northern Ireland, the SAR should be dealt with by the school. If the school is in Scotland, the SAR should be dealt with by the relevant education authority or the proprietor of an independent school.

It should be noted that there are two distinct rights to information held about pupils by schools. They are:

- the pupil's right of subject access under GDPR; and
- the parent's right of access to their child's 'educational record'.

The following should also be noted:

- Only children aged 13 or over are able provide their own consent. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- For children under this age you consent is required from whoever holds parental responsibility for the child

Although this code is only concerned with the operation of the right of subject access, it is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above, and also because this concept is relevant when ascertaining the amount of the fee which may be charged for responding to a SAR.

The statutory definition of 'educational record' differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of that pupil's educational record. However, it is possible that some of the information could fall outside of the educational record, e.g. information about the pupil provided by the parent of another child is not part of the educational record.

For more detailed guidance about what information forms part of the educational record, and about a parent's right of access to that record, see ICO guidance for each jurisdiction.

Unlike the right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf, by virtue of age, or has given their consent. If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, this should be clarified before responding to the SAR.

In deciding what information to supply in response to a SAR, it is necessary to have regard to the general principles about exemptions from subject access described elsewhere in this code. Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

- information which might cause serious harm to the physical or mental health of the pupil or another individual;
- information which would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records, and;
- certain information given to a court in proceedings concerning the child.

If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days (if the school is in England, Wales or Northern Ireland) and the maximum amount that may be charged for dealing with the request depends upon the number of pages of information which are to be supplied

Enforcing the right of subject access

The Information Commissioner's enforcement powers

Anyone who believes they are directly affected by the processing of personal data may ask the Information Commissioner's Office (ICO) to assess whether it is likely or unlikely that such processing complies with the Data Protection Act 1998 (DPA). This is called a compliance assessment.

If our assessment is that it is likely that an organisation has failed to comply with GDPR (or is failing to do so), we may ask it to take steps to comply with the data protection principles. Where appropriate, the ICO may order the organisation to do so. However, the ICO has no power to award compensation to individuals – only the courts can do this.

The Information Commissioner may serve an enforcement notice if he is satisfied that an organisation has failed to comply with the subject access provisions. An enforcement notice may require an organisation to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence.

The Information Commissioner has a statutory power to impose a financial penalty on an organisation if he is satisfied that the organisation has committed a serious breach of GDPR which is likely to cause substantial damage or distress.

For more information about the Information Commissioner's enforcement powers, see the 'ICO Guide to Data Protection'.

Enforcement by court order

If the school fail to comply with a subject access request (SAR), the requester may apply for a court order requiring us to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

The courts have indicated that, where other legal proceedings are contemplated or in progress, they may be reluctant to allow individuals to use the right of subject access as a means of accessing information in connection with those proceedings where disclosure should more appropriately be dealt with under the Civil Procedure Rules. The courts may even regard an application for an order under GDPR to be an 'abuse of process' if the application would not have been made but for the desire to access information to be used in other legal proceedings. Nevertheless, as explained in chapter 9, whether or not a court would be likely to grant an enforcement order has no bearing on

our legal duty to comply with a SAR. The school may only refuse to comply if a relevant exemption under GDPR applies in the circumstances of the request.

Awards of compensation

If an individual suffers damage because the school have breached GDPR – including, of course, by failing to comply with a SAR – they are entitled to claim compensation from the school. This right can only be enforced through the courts. GDPR allows the school to defend a claim for compensation on the basis that The school took all reasonable care in the circumstances to avoid the breach, but it is likely to be difficult to establish this defence where the school have failed to respond to a SAR within the prescribed time limit, or where the school have not provided the requester with all the information to which they are entitled.