satswana

Company registered number 09329065 www.satswana.com

Satswana Paper for Schools on FOI and SAR Requests

Introduction

This paper is intended to bring together the experience gained in handling subject access requests, it also applies to freedom of information requests since the two are closely aligned both in regulatory and precedent terms. DPA 2018 actually requires that GDPR provisions apply to FOI data. Whilst at the date of publication it is the best information that we have to hand, please be aware that case law, precedents, and decisions of the Information Commissioners Office will mean continuous change to actual practice. Please reconfirm any statements made or positions suggested before relying on them.

It is important to consider the requested information under the right legislation, this is because a disclosure under FOIA/FOISA or the EIR/EIRs is to the world at large – not just the requester. A Subject Access Request is for the attention of the individual. If personal data is mistakenly disclosed under FOIA/FOISA or the EIR/EIRs, this could lead to a personal data breach. It is recommended that you generally default to treating an access request as a SAR.

The new statutory exemptions are, as yet, un-litigated, but many are a continuation of those under the Data Protection Act 1998. This means that case law under the previous data protection regime will often still be relevant under the GDPR.

Areas such as litigation privilege, the mixed data exemption, the extent of the search which must be undertaken and the degree of effort which must be made, as well as the relevance of the motive behind the SAR, have been litigated with results which are not always in line with the regulator's views. The outcomes of these cases may need to be considered when responding to a complex SAR.

The document has seven basic parts as follows

A Do I have to answer?

B Guide to exemptions

C Exemptions

D Excluded Emails

E Safeguarding

F Vexatious aspects

G Further detailed ICO guidance

A Do I have to answer?

Generally yes but there are exceptions, which we will cover below. The idea was to increase transparency and reduce executive secrecy, so there will be occasions where you will support an information hunting exercise.

However within schools the requests have also become a weapon of choice for certain categories of applicants, normally looking for ammunition to use against you. Those circumstances can become very stressful for staff so you should contact us for help. We only ever do what you tell us to do, as is appropriate for a peripatetic member of your staff, which is our status. But we are doing these all the time, and you should ask us to take the load.

Two quick important points, the first being that a request does not have to be in writing, so please assume it is a valid request if any words are used that you interpret to have that meaning. Second, you must respond within 30 days, but please note that acknowledging the request is adequate as a response. You will find many lawyers stating that you must provide the full answer within the time period, that is not so!!

1 When can I refuse to answer?

Please bear in mind that if you do refuse to respond then the applicant has the right to complain to the ICO by using the procedure here. https://ico.org.uk/make-a-complaint/ - indeed if you do reply (and you will see one instance where we recommend you do not) then you should advise them of their right to challenge your decision if you are not providing a full answer. You must be ready and prepared to support the reason for your decision to the ICO. (If you do not accept my finding then you have the right to use the Complaints procedure of the Information Commissioners Office, details of which you will find here https://ico.org.uk/make-a-complaint/)

2 I only wanted somebody to talk to me

We have lost count of the number of requests that have been resolved by simply creating communications with the applicant. Very often a misunderstanding can build up that can be entirely defused in seconds, try that first!

3 A Clear "marketing" misuse of data

We have seen examples of clear selling motives dressed up as requests, a notable one being of the energy use at a school. We recommend that these are totally ignored, do not respond to the email as it just validates that the address is correct, whereas they may have guessed it.

4 Where the person is not identified

You have the right to know who you are dealing with, so just having a name at Gmail.com for instance, could be (and may well be) an alias. You will also find people using various forms of what we describe as "campaigning" websites where the email address refers to the

site and you have no confirmation of the name used. We believe these sites to be predatory, in that they seek "donations" for their use. Moreover in publicising their results they tend to reveal the personal data of those replying. We normally advise against a response, but you will get automated follow ups, ignore those as well. If the ICO instruct you to answer, then you will have to do so, but then the identity will be authenticated.

5 Where a request is unjustified, or repetitive

Using this exception will turn on the facts of the individual case, but the ICO have been known to support schools who respond in the following terms. "I must advise you that the School is entitled to refuse to answer requests that are manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. It is my belief that any further correspondence has the potential to cause a disproportionate or unjustified level of disruption, irritation or distress to the School as a publicly funded body as defined in case law when considering the issue of vexatious processes." You do not have to use all those sentences, only those that apply. (See G 16) In an alternative to straight refusal you can request a reasonable fee. See further explanation from ICO guidance at G 8, and G20 below

6 Cost and time

Similarly the ICO have supported circumstances where the cost and time of preparing a response is out of all proportion to the value or the importance of the data requested. Schools have responded that "it would cost too much and take too much time from our scarce resources to provide an answer in the terms requested". Prior to using this defence we advise requesting that the applicant narrows the range of their request, either by date or subject, for instance.

7 Disruption, irritation or distress?

See the section on vexatious requests for more but Section 14(1) is designed to protect public authorities by allowing them to refuse any requests which have the potential to cause a disproportionate or unjustified level of disruption, irritation or distress. (Section F)

B Guide to Exemptions from Subject Access Requests

The following information is taken from guidance provided by the Information Commissioners Office and is intended to be a precis of exemptions that may routinely apply to Education. Since it is a precis, if you are in any doubt on any matter, please refer to the original content that can be found here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

The GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances.

Whether or not you can rely on an exemption often depends on why you process personal data.

You should not routinely rely on exemptions; you should consider them on a case-by-case basis.

You should justify and document your reasons for relying on an exemption.
If no exemption covers what you do with personal data, you need to comply with the GDPR as normal.

1 Checklists

Consider whether you can rely on an exemption on a case-by-case basis.

Carefully consider the extent to which the relevant GDPR requirements would be likely to prevent, seriously impair, or prejudice the achievement of your processing purposes.

Justify and document the reasons for relying on an exemption.

(When an exemption does not apply [or no longer applies] to your processing of personal data, you must comply with the GDPR's requirements as normal.)

2 Some things are not exemptions.

This is simply because they are not covered by the GDPR. Here are some examples:

a) Domestic purposes – personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity is outside the GDPR's scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the GDPR.

b) Law enforcement – the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018. See the Guide to Law Enforcement Processing for further information.

c) National security – personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the 'applied GDPR'), which contains an exemption for national security and defence.

3 Some exemptions apply simply because you have a particular purpose.

But others only apply to the extent that complying with the GDPR would:

a) Be likely to prejudice your purpose (e.g. have a damaging or detrimental effect on what you are doing); or

b) Prevent or seriously impair you from processing personal data in a way that is required or necessary for your purpose.

c) Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis.

If an exemption does apply, sometimes you will be obliged to rely on it (for instance, if complying with GDPR would break another law), but sometimes you can choose whether or not to rely on it.
In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance.

C Exemptions

1 Legal professional privilege, Schedule 2, Part 4, Paragraph 19, This exemption applies if you process personal data: to which a claim to legal professional privilege (or confidentiality of communications in Scotland) could be maintained in legal proceedings;

a) Or in respect of which a duty of confidentiality is owed by a professional legal adviser to his client. (Please note this is much wider than just a lawyer or barrister and could be the Police for instance.)

b) Is of the type which would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders if disclosed.

2 Self-incrimination, Schedule 2, Part 4, Paragraph 20, this exemption can apply if complying with the GDPR provisions below would reveal evidence that you have committed an offence. The exemption only applies to the extent that complying with these provisions would expose you to proceedings for the offence.

3 Protection of the rights of others, paragraphs 16 and 17 of schedule 2, Part 3 of the DPA 2018.

There is an exemption in the DPA 2018 that says you 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 to comply with the request without that individual's consent.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision involves 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 you disclosing the information about them, it is unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

You can say the School does not have consent from these parents to share their emails or record of meeting notes. School considered the disclosure of these documents a breach of other parents' data protection rights. (Consent data would normally be within your Privacy Policy.)

You may only disclose the information about the third party where they have consented to the disclosure or where it is reasonable to disclose the information without their consent.

DPA18 sets out that what needs to be taken into account when assessing whether or not it is reasonable to disclose third party information, it includes:

a) The type of information you would disclose.

b) Any duty of confidentiality you owe to the other individual.

c) Any steps you have taken to seek consent from the other individual.

d) Whether the other individual is capable of giving consent. And

e) Any express refusal of consent by the other individual.

Essentially the decision involves balancing the competing rights of the individuals involved. Case law (which remains relevant under the new regime) suggests that the controller has a wide margin of assessment and a wide discretion as to which factors to treat as relevant. In a 'tie-breaker' situation, presumption will fall in favour of non-disclosure

(ICO guidance, How do we identify someone indirectly?)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/can-we-identify-an-individual-indirectly/)

Extract from above link. It's important to be aware that information you hold may indirectly identify an individual and therefore can still be personal data. If so, this means that the information is subject to the GDPR.

If you cannot identify an individual directly from the information that you are processing (for example where all identifiers have been removed) an individual may still be identifiable by other means. This may be from information you already hold, or information that you need to obtain from another source. Similarly, a third party (this could be a person making a subject access request) could use information you process and combine it with other information available to them.

You must carefully consider all of the means that any party is reasonably likely to use to identify that individual. This is important because you could inadvertently release or disclose information that could be linked with other information and (inappropriately) identify an individual.

4 Social work data, an individual's expectation and wishes, Schedule 3 Part 3, Paragraph 10, exemption applies to the extent that complying with the request would disclose information that:

a) The individual provided in the expectation that it would not be disclosed to the requestor, unless the individual has since expressly indicated that they no longer have that expectation;

b) Was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or

c) The individual has expressly indicated should not be disclosed in this way.

See also G25

5 Social work data, schedule 3, Part 3, Paragraph 11. School considered that complying with the right of access would be likely to prejudice carrying out social work because it would be likely to cause serious harm to the physical or mental health of an individual. See also G 26

6 Health data – an individual's expectations and wishes, Schedule 3, Part 2,

Paragraph 4, the exemption only applies to the extent that complying with the request would disclose information that:

a) The individual provided in the expectation that it would not be disclosed to the requestor, unless the individual has since expressly indicated that they no longer have that expectation;

b) Was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or

c) The individual has expressly indicated should not be disclosed in this way.

See also G21

7 Health data – serious harm, Schedule 3, Part 2, Paragraph 5 the exemption only applies to the extent that compliance with the right of access would be likely to cause *serious harm* to the *physical* or *mental health* of any individual. This is known as the 'serious harm test' for health data.

You can only rely on this exemption if within the last six months you have obtained an opinion from an appropriate health professional that the serious harm test for health data is met.

Health data, restriction of right to access, Schedule 3, Part 2, Paragraph 6, restriction from disclosing health data unless

a) You are a health professional; or

b) Within the last six months you have obtained an opinion from an appropriate health professional that the serious harm test for health data is not met. Even if you have done this, you must re-consult the appropriate health professional if it would be reasonable in all the circumstances.

See also G22

8 Child abuse data, Schedule 3 Part 5, complying with the request would not be in the best interests of the individual who the child abuse data is about. See also G 19.

9 Negotiations, Schedule 2, Part 4, Paragraph 23, exemption can apply to personal data in records of your intentions relating to any negotiations with an individual. The subject is not entitled to personal data which consists of a record of the employer's intentions in respect of settlement discussions that have taken place or are in the process of taking place with that individual.

10 Confidential references, Schedule 2, Part 4, Paragraph 24. Exemption applies if you give or receive a confidential reference for the purposes of prospective or actual:

a) Education, training or employment of an individual;

b) Placement of an individual as a volunteer;

c) Appointment of an individual to office; or

d) Provision by an individual of any service.

11 Exam scripts or exam marks, Schedule 2, Part 4, Paragraph 25, applies to the information recorded by candidates. This means candidates do not have the right to copies of their answers to the exam questions.

12 Education data – serious harm, Schedule 3, Part 4, Paragraph 19, exempts you from the GDPR's provisions on the right of access regarding your processing of education data. But the exemption only applies to the extent that complying with the right of access would be likely to cause serious harm to the physical or mental health of any individual. (This is known as the 'serious harm test' for education data.)

13 University of Worcester precedent

Further to the decision of the Commissioner in the case of the University of Worcester, information was excluded that would otherwise inhibit a free and frank exchange of views for the purposes of deliberation where it consisted of a personal exchange between professionals. This is not part of the Regulation but is a precedent established by the Commissioner's decision.

14 Confidential references

Employers do not have to provide subject access to references they have confidentially given in relation to an employee's employment. (This was a specific addition to DPA 2018 and varies from GDPR 2016.)

15 Management information

Personal data which relates to management forecasting or planning is exempt from subject access (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation).

D Excluded emails, Schedule 2, Part 3, Paragraph 16.

a) Where emails were between the school and the applicant it was considered that they already had the information so duplicates were not provided.

b) Where they are either email correspondence from other parents in relation to incidents and concerns involving the applicant's Child or a record of meetings held with other parents where the Child's name was mentioned.

c) Where they should be withheld in order to protect certain individuals (parents and children) as they contain confidential information specific to parental views or personal information about other children.

d) Where disclosing documents would compromise the identity of individuals in those documents. Redacting personal data in these documents would not be adequate to protect their identity. (Parents and children would remain identifiable from timings, dates, incidents and the nature of the school setting)

See also G 10

E Safeguarding

You will note that many of the exemptions in **C** above could be used in safeguarding circumstances and there may be very special circumstances where you might use them extensively. For instance there was a situation where the School was convinced that the applicant had mental health issues, and the correspondence between agencies would have disclosed the discussion of that belief. In a situation of unconfirmed diagnoses, can you possibly give that information to the person? Clearly no!

1 Keeping children safe in education – 2019

The Information sharing section of this act starts at Article 76, through 83 and any consideration of data sharing should be aware of these provisions, not least because Article 78 expressly states: "The Data Protection Act 2018 and GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children."

2 Nonspecific information

An example of a clause we have seen in reporting the exemption of data is as follows: "we did not provide copies where documents do not contain safeguarding information relating specifically to the applicant's Child. The School are therefore not withholding safeguarding information about the Child."

3 Child Abuse Data,

Exemption from Article 15 of the GDPR: child abuse data, DPA 2018, Schedule 3, Part 5

21(1) this paragraph applies where a request for child abuse data is made in exercise of a power conferred by an enactment or rule of law and—

a) The data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject, or

b) The data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to child abuse data to the extent that the application of that provision would not be in the best interests of the data subject.

(3) "Child abuse data" is personal data consisting of information as to whether the data subject is or has been the subject of**,** or may be at risk of, child abuse.

(4) For this purpose, "child abuse" includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18.

F Vexatious aspects

This is actually taken from FOI case law, but it applied back to DPA 1998, and substantively carries over into DPA 2018, at least we believe that the precedents would have a very strong influence on a Court.

Whether or not an applicant is vexatious has to be an aspect that is considered in some cases, but is very rarely something upon which the parties are going to agree. It is an unfortunate reality that an applicant can become aggrieved to the point of sometimes extreme abuse, whereas simply nothing that the school can do will ever satisfy them. Since

the parties are so polarised almost the only option open is for the school to draw a line. You will then have to leave it to some other form of adjudication to decide who is right, and one form available is the complaints procedure of the ICO.

1 Disruption, irritation or distress defence

We believe this is best executed by the defence previously mentioned using Section 14 (1) since a school is a public authority. You can refuse any requests which have "the potential to cause a disproportionate or unjustified level of disruption, irritation or distress."

2 Definition

This heading seeks to highlight cases where the definition of vexatious has been established.

Vexatious has one definition below. (Italics for emphasis)

The full text of the ICO advice in the matter can be found here…

https://ico.org.uk/media/1198/dealing-with-vexatious-requests.pdf

But to extract the essence

The meaning of vexatious

In Information Commissioner vs Devon County Council & Dransfield [2012]UKUT440(AAC), (28 January 2013)the Upper Tribunal took the view that the ordinary dictionary definition of the word vexatious is only of limited use, *because the question of whether a request is vexatious ultimately depends upon the circumstances surrounding that request.*

In further exploring the role played by circumstances, the Tribunal placed particular emphasis on the issue of whether the request has adequate or proper justification. They also cited two previous section 14(1) decisions where the lack of proportionality in the requester's previous dealings with the authority was deemed to be a relevant consideration by the First Tier Tribunal.

After taking these factors into account, the Tribunal concluded that 'vexatious' could be defined as the"...*manifestly unjustified, inappropriate or improper use of a formal procedure.'*

The Tribunal's decision clearly establishes that the concepts of 'proportionality 'and 'justification' are central to any consideration of whether a request is vexatious.

At the subsequent Court of Appeal Case (Dransfield v Information Commissioner and Devon County Council [2015]EWCA Civ454 (14 May 2015)), Lady Judge Arden observed that;"...the emphasis should be on an objective standard and that the starting point is that vexatiousness primarily involves *making a request which has no reasonable foundation, that is, no reasonable foundation for thinking that the information sought would be of value to the requester or to the public or any section of the public."* (Para 68)

G Further detailed ICO Guidance

This Guide had already been written when a most welcome and comprehensive version was provided by the ICO. The headings below are taken from that document and add subject matter and detail. In places guidance is duplicated, but it is included nonetheless.

1 Who can make an Access Request?

Generally the applicant themselves will make the request, but if it does come from a third party we recommend that you receive confirmation directly from the applicant. We do not accept an authority forwarded by a Solicitor for instance, we wish to have absolute proof that the applicant consents.

2 Can a request be made on behalf of someone?

An individual may prefer a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf. The GDPR does not prevent this; however you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this. This might be a written authority to make the request or a more general power of attorney.

In most cases, provided you are satisfied that the third party has the appropriate authority, you should respond directly to that third party. However, if you think an individual may not understand what information would be disclosed, and in particular you are concerned about disclosing excessive information, you should contact the individual first to make them aware of your concerns. If the individual agrees, you may send the response directly to them rather than to the third party. The individual may then choose to share the information with the third party after reviewing it. If you cannot contact the individual you should provide the requested information to the third party (as long as you are satisfied that they are authorised to act on the individual's behalf). If you are processing health data please see 'What about requests for health data from a third party?' There are cases where an individual does not have the mental capacity to manage their own affairs. There are no specific provisions in the GDPR, the Mental Capacity Act 2005, the Mental Capacity Act (Northern Ireland) 2016 (please note that not all provisions in the Act have been commenced at this time) or in the Adults with Incapacity (Scotland) Act 2000 which enable a third party to exercise subject access rights on behalf of such an individual.

3 Do we have to respond to requests made via a third party online portal?

You may receive a SAR made on behalf of an individual through an online portal, for example a third party that provides services to assist individuals in exercising their rights.

To determine whether you must comply with such a request, you need to consider if you:

have been made aware that a particular individual is exercising their rights under Article 15;

are able to verify the identity of the individual, if this is in doubt we ask for ID.

are satisfied the third party portal is acting with the authority of, and on behalf of, the individual.

You are not obliged to take proactive steps to discover that a SAR has been made. Therefore, if you cannot view a SAR without paying a fee or signing up to a service, you have not 'received' the SAR and are not obliged to respond. You should note that it is the portal's responsibility to provide evidence that it has appropriate authority to act on the individual's behalf. Mere reference to the terms and conditions of its service are unlikely to be sufficient for this purpose (see 'Can a request be made on behalf of someone?' above). The portal should provide this evidence when it makes the request (i.e. in the same way as other third parties). When responding to a SAR, you are also not obliged to pay a fee or sign up to any third party service. If you are in this position you should instead provide the information directly to the individual.

4 Right of a Child

What about requests for information about children or young people?

Even if a child is too young to understand the implications of the right of access, it is still their right. Even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them, it is still the right of the child rather than anyone else's.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive. When considering borderline cases, you should take into account, among other things:

a) the child's level of maturity and their ability to make decisions like this;

b) the nature of the personal data;

c) any court orders relating to parental access or responsibility that may apply;

d) any duty of confidence owed to the child or young person;

e) any consequences of allowing those with parental responsibility access to the child or young person's information (this is particularly important if there have been allegations of abuse or ill treatment);

f) any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

g) any views the child or young person has on whether their parents should have access to information about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This does not apply in England, Wales or Northern Ireland but would be a reasonable starting point.

5 There are two distinct rights to information held about pupils by schools:

The pupil's right of access under Article 15 of the GDPR; and Relevant provisions in the DPA 2018 See Schedule 3, Part 4, paragraphs 13-17

The parent's right of access to their child's 'educational record'. In England, Wales and Northern Ireland this right of access is only relevant to maintained schools (all grant aided schools in Northern Ireland) – not independent schools, academies or free schools. However in Scotland the right extends to all schools.

Although this guidance is only concerned with the right of access under the GDPR, it is important to be aware of a parent's right to access their child's educational records. This is because the information you provide may differ depending on which right applies, i.e. the parent's right is only to access their child's educational record, whereas a SAR also enables access to personal data processed by a school that does not fall into the definition of an educational record. The two rights also have different time limits for compliance. You must respond to a parent's right of access to their child's educational records within 15 school days, whereas you must comply with a SAR within one month. The law on a parent's right to their child's educational records does not lie within the regulatory responsibilities of the ICO, but we refer to it here for completeness.

Unlike the parent's right of access to their child's educational record, the right to make a SAR is the pupil's right. Parents are only entitled to submit a SAR for information about their child if the child is not competent to act on their own behalf 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, you should clarify this before responding to the SAR. If the school is in England, Wales or Northern Ireland, the school should deal with the SAR. If the school is in Scotland, the relevant education authority or the proprietor of an independent school should deal with the SAR.

Although this guidance is only concerned with the right of access under the GDPR, it is important to be aware of a parent's right to access their child's educational records. This is because the information you provide may differ depending on which right applies, i.e. the parent's right is only to access their child's educational record, whereas a SAR also enables access to personal data processed by a school that does not fall into the definition of an educational record. The two rights also have different time limits for compliance. You must respond to a parent's right of access to their child's educational records within 15 school days, whereas you must comply with a SAR within one month. The law on a parent's right to their child's educational records does not lie within the regulatory responsibilities of the ICO, but we refer to it here for completeness.

Unlike the parent's right of access to their child's educational record, the right to make a SAR is the pupil's right. Parents are only entitled to submit a SAR for information about their child if the child is not competent to act on their own behalf 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, you should clarify this before responding to the SAR. If the school is in England, Wales or Northern Ireland, the school should deal with the SAR. If the school is in Scotland, the relevant education authority or the proprietor of an independent school should deal with the SAR.

6 Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is: complex; or you have received a number of requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.

You should calculate the extension as three months from the original start date, i.e. the day you receive the request, fee or other requested information.

7 When is a request complex?

Whether a request is complex depends upon the specific circumstances of each case. What may be complex for one controller may not be for another – the size and resources of an organisation are likely to be relevant factors. Therefore, you need to take into account your specific circumstances and the particular request when determining whether the request is complex.

The following are examples of factors that may in some circumstances add to the complexity of a request. However, you need to be able to demonstrate why the request is complex in the particular circumstances.

• Technical difficulties in retrieving the information – for example if data is electronically archived.

• Applying an exemption that involves large volumes of particularly sensitive information.

• Clarifying potential issues around disclosing information about a child to a legal guardian.

• Any specialist work involved in redacting information or communicating it in an intelligible form.

Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual has requested a large amount of information.

Also, a request is not complex just because you have to rely on a processor to provide the information you need in order to respond.

8 Can we charge a fee?

In most cases you cannot charge a fee to comply with a SAR. However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if: it is manifestly unfounded or excessive; or an individual requests further copies of their data following a request. (For values see G 20)

9 Can we clarify the request?

If you process a large amount of information about an individual, you may ask them to specify the information or processing activities their request relates to before responding to the request. However, this does not affect the timescale for responding - you must still respond to their request within one month. You may be able to extend the time limit by two months if the request is complex or the individual has made a number of requests.

Information is 'deleted' when you try to permanently discard it and you have no intention of ever trying to access it again. The ICO's view is that, if you delete personal data held in electronic form by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean you must go to such efforts to respond to a SAR.

The ICO will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form. We do not require organisations to use time and effort reconstituting information that they have deleted as part of their general records management.

10 What about information contained in emails?

The contents of emails stored on your computer systems are a form of electronic record to which the general principles above apply. For the avoidance of doubt, you should not regard the contents of an email as deleted merely because it has been moved to a user's 'Deleted items' folder.

It may be particularly difficult to find information related to a SAR if it is contained in emails that have been archived and removed from your 'live' systems. Nevertheless, the right of access is not limited to personal data that is easy for you to provide. You may, of course, ask the requester to give you some context that would help you find what they want if you process a large amount of information about them.

11 What about information stored on personal computer equipment?

You are only obliged to provide personal data in response to a SAR if you are a controller for that data. In most cases, therefore, you do not have to supply personal data if it is stored on someone else's computer systems rather than your own (the exception being where that person is a processor). However, this may not be the case if the requester's personal data is

stored on equipment belonging to your staff (such as smartphones or home computers) or in private email accounts.

It is good practice to have a policy restricting the circumstances in which staff may hold information about customers, contacts or other employees on their own devices or in private email accounts. Some organisations enable staff to access their systems remotely (e.g. via a secure website), but most are likely to prohibit the holding of personal data on equipment the organisation does not control. Nevertheless, if you do permit staff to hold personal data on their own devices, they may be processing that data on your behalf, in which case it is within the scope of a SAR you receive. The purpose for which the information is held, and its context, is likely to be relevant. We do not expect you to instruct staff to search their private emails

12 What about other records?

If you hold information about the requester in non-electronic form (e.g. in paper files or on microfiche records), you need to decide whether it is covered by the right of access. You need to make a similar decision if you have removed electronic records from your live systems and archived them in non-electronic form.

Whether the information in such hard-copy records is personal data accessible via the right of access depends primarily on whether the non-electronic records are held in a 'filing system'. This is because the GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'.

However, under the DPA 2018 personal data held in unstructured manual records processed by public authorities is covered by the right of access. This includes paper records that are not held as part of a filing system. Therefore, public authorities may have to search this information to comply with SARs.

13 Can we amend data following receipt of a SAR?

It is the ICO view 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 you are dealing with the request. So it is reasonable for you to supply the information you hold when you respond, even if this is different to what you held when you received the request. However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under the DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure.

14 Do we need to provide remote access?

The GDPR encourages controllers to provide individuals with remote access to their personal data via a secure system.

This is not appropriate for all organisations, but there are some sectors where this may work well. It also helps you to meet your obligations, and reassure individuals about the amount and type of personal data you hold about them.

You should note however that although you have provided them with access to their personal data, it does not necessarily mean that you have provided them with a copy of their data. This depends on whether they are able to download of copy of the information they have requested. If an individual can download a copy of their personal data in a commonly used electronic format, then this satisfies the requirement to provide a copy, as long as the individual does not object to the format.

15 What if we have also received a data portability request?

If an individual makes a SAR and a request for data portability at the same time, you need to consider what information comes under the scope of the SAR and what information comes under the scope of the data portability request.

An easy way of considering this is to remember that:

• the right of access concerns all the personal data you hold about an individual (unless an exemption applies) – including any observed or inferred data; and

• the right to data portability only applies to personal data 'provided by' the individual, where you process that data (by automated means) on the basis of consent or contract.

Also, whilst the right of access may require you to provide information in a commonly used electronic format, the right to data portability goes further. It gives individuals the right to receive personal data they have provided to you in a structured, commonly used and machine readable format. It also gives them the right to request that you transfer this data directly to another controller.

16 Further explanation of manifestly unfounded or excessive

You should consider each request on a case-by-case basis in order to decide if it is manifestly unfounded or excessive. You should not have a blanket policy. You must be able to demonstrate to the individual why you consider that the request is manifestly unfounded or excessive and, if asked, explain your reasons to the ICO.

a) What does manifestly unfounded mean?

A request may be manifestly unfounded if the individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:

Where the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption; or the request makes unsubstantiated accusations against you or specific employees; the individual is targeting a particular employee against whom they have some personal grudge; or the individual systematically sends different

requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded. Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language. The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request is manifestly unfounded.

b) What does excessive mean?

A request may be excessive if it: repeats the substance of previous requests and a reasonable interval has not elapsed; or it overlaps with other requests. However, it depends on the particular circumstances. It is not necessarily excessive just because the individual requested a large amount of information, even if you might find the request burdensome (instead you should consider asking them for more information to help you locate what they want to receive); wanted to receive a further copy of information they have requested previously (instead you can charge a reasonable fee for the administrative costs of providing this information again); made an overlapping request relating to a completely separate set of information; or previously submitted requests which have been manifestly unfounded or excessive.

When deciding whether a reasonable interval has elapsed you should consider: the nature of the data – this could include whether it is particularly sensitive; the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed; and how often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this.

17 Confidentiality

Confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third-party without their consent. A duty of confidence arises where information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to you with the expectation it remains 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: Medical (doctor and patient), Employment (employer and employee), Legal (solicitor and client), Financial (bank and customer), Caring (counsellor and client)

However, you 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 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 is usually reasonable to withhold third-party information, unless you have the third-party individual's consent to disclose it.

18 Workers Health, Safety and Welfare

To secure workers' health, safety and welfare or to protect others against health and safety risks in connection with (or arising from) someone at work

If you rely upon this exemption and the individual makes a complaint to the ICO, we expect you to be able to explain why the exemption is required in each case, and how and by whom this was considered at the time. The ICO does not have to agree with your view – but we must be satisfied that you had a reasonable belief.

19 Child abuse data

Child abuse data is personal data consisting of information about whether the data subject is or has been the subject of, or may be at risk of, child abuse. This includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18.

You are exempt from providing child abuse data in response to a SAR if you receive a request (in exercise of a power conferred by an enactment or rule of law) from someone: with parental responsibility for an individual aged under 18; or appointed by court to manage the affairs of an individual who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would not be in the best interests of the individual concerned (i.e. the person the child abuse data relates to).

20 Unstructured manual records

The GDPR does not cover non-automated information which is not, or is not intended to be, part of a 'filing system'. However, under the DPA 2018 unstructured manual information processed by public authorities constitutes personal data. This includes paper records that are not held as part of a filing system. Therefore, public authorities may have to search such information to comply with a SAR. However, they are not obliged to do so if:

a) the request does not contain a description of the unstructured data; or

b) it is estimated that the cost of complying with the request would exceed the appropriate maximum.

The “appropriate maximum” is currently £600 for central government, Parliament and the armed forces and £450 for all other public authorities. Please note that in Scotland the appropriate maximum is £600 for all public authorities.

The biggest cost is likely to be staff time. You should rate staff time at £25 per person per hour, regardless of who does the work, including external contractors. This means a limit of 18 or 24 staff hours, depending on whether the £450 or £600 limit applies to your public authority. For further information, please see the Fees Regulations.

21 Is health data exempt -

if disclosure goes against an individual’s expectations and wishes?

There is an exemption from the right of access if you receive a request (in exercise of a power conferred by an enactment or rule of law) for health data from someone:

a) with parental responsibility for an individual aged under 18 (or 16 in Scotland); or

b) appointed by the court to manage the affairs of an individual who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would disclose information that: Relevant provisions in the DPA 2018 (the exemption) See Schedule 3, Part 2, Paragraph 3 Relevant provisions in the GDPR (the exempt provisions) See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)(2), 18(1), 20(1)-(2), 21(1)

The individual had provided to you in the expectation that it would not be disclosed to the requester, unless the individual has since expressly indicated that they no longer have that expectation; was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or the individual has expressly indicated should not be disclosed in this way.

22 Is health data exempt if disclosure could cause serious harm?

You are exempt from complying with a SAR for health data to the extent that complying with the right of access would be likely to cause serious harm to the physical or mental health of any individual. This is known as the ‘serious harm test’ for health data.

You can only rely on this exemption if:

a) you are a health professional; or

b) within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health data is met. Even if you have done this, you still cannot rely on the exemption if it would be reasonable in all the circumstances to reconsult the appropriate health professional.

The appropriate health professional is the health professional most recently responsible for the diagnosis, care or treatment of the individual. If the most recent health professional no longer practices, you can appoint a health professional with the necessary experience and expertise.

23 What is education data?

The DPA 2018 defines 'education data' as: personal data which consists of information that forms part of an educational record; but is not health data.

The definition of 'educational record' in the DPA 2018 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. The definition applies to nearly all schools including maintained schools, independent schools and academies.

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 forms part of the pupil's educational record. However it is possible that some of the information could fall outside the educational record, eg information about the pupil provided by the parent of another child is not part of the educational record.
How can education data be accessed?

24 Is education data exempt if disclosure could cause serious harm?

You are exempt from providing education data in response to a SAR to the extent that complying with the request would be likely to cause serious harm to the physical or mental health of any individual. This is known as the 'serious harm test' for education data.

25 Is social work data exempt

if disclosure goes against an individual's expectations and wishes?

There is an exemption from the right of access if you receive a request (in exercise of a power conferred by an enactment or rule of law) for social work data concerning an individual from:

a) someone with parental responsibility for an individual aged under 18 (or 16 in Scotland); or

b) someone appointed by court to manage the affairs of an individual who is incapable of managing their own affairs.

Relevant provisions in the DPA 2018 (the exemption) See Schedule 3, Part 3, Paragraph 9
Relevant provisions in the GDPR (the exempt provisions) See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)(2), 18(1), 20(1)-(2), 21(1)

But the exemption only applies to the extent that complying with the request would disclose information that: the individual provided in the expectation that it would not be disclosed to the requester, unless the individual has since expressly indicated that they no longer have that expectation; was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or the individual has expressly indicated should not be disclosed in this way.

26 Is social work data exempt if disclosure could cause serious harm?

You are exempt from complying with a SAR for social work data to the extent that complying with the request would be likely to prejudice carrying out social work because it would be likely to cause serious harm to the physical or mental health of any individual. This is known as the 'serious harm test' for social work data.

27 Can a SAR be enforced by a court order?

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

28 Can an individual be awarded compensation?

If an individual suffers damage or distress because you have infringed their rights under the data protection legislation – including, of course, by failing to comply with a SAR – they are entitled to claim compensation from you. This right can only be enforced through the courts. You will not be liable if you can prove that you are not in any way responsible for the event giving rise to the damage.

29 Is it a criminal offence to destroy and conceal information?

It is a criminal offence, in certain circumstances, to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR would have been entitled to receive.