This document is a combined representation of views from the organisations that fall within a North West Data Protection Group.

The group consists of different organisations include local authorities, housing associations, charities and universities and includes data protection officers and information governance managers.

At our recent meeting, we discussed the consultation and agreed that instead of the ICO receiving a number of individual representations that we would consolidate the response into one.

General Comment

The guidance seems to wrongly suggests, right from the start, that the right gives individuals the right to obtain "a copy of their personal data". This is not legally accurate or true. Whilst copies of information are commonly provided in response to a request (as this if often the best way to provide access) the right is a right of *access*, not a right to copies- 45 2) g) "communication of the personal data undergoing processing and of any available information as to its origin" -is how it is set out in the DPA 2018. Communication of the information may not necessarily involve providing copies, especially where images are involved and access may be offered via an appointment to view rather than providing copies or it is difficult to give copies. This inaccuracy is repeated on p.29 and page 30 where it says "you must provide the requestor with a copy". There is a nod to the correct interpretation on page 30 where it says: "The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents" but this contradicts what has been said before and is confusing.

Page 7: Your systems should also be designed to allow you to redact third party data where necessary.

This is easier said than done. Not all systems have been designed with this in mind as yet. It may need investment to use third party products to implement this as and when required.

I'm surprised that under Security the ICO just says (page 7) "Security – Have measures in place to securely send information. For example, by using a trusted courier or having a system to check email addresses before sending." I think more could be said about sending via a secure rather than standard email and whether they recommend recorded or special delivery as well and encrypting data in transit where necessary, especially given that if security is not sufficient enough this could result in a personal data breach.

Would be useful for some guidance on what methods can be used for redaction, eg hard to get the budget to buy specific software for all to use so having something that's mandated as a standard would be beneficial

Page 9:-Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted

It would be helpful to be able to ask requestors to follow up in writing in order to ensure we have correctly documented their requirement and to provide an audit trail as over the phone, it is not possible to get every point noted down. I did ask the ICO in 2019 if we could ask for things to be put in writing and was informed that we could

Page 9:- In most circumstances it will not be appropriate to use social media to supply information in response to a SAR for information security reasons. Instead you should ask for an alternative delivery address for the response.

If they refuse to provide it, can we then refuse to provide the information as it's over a non-secure method?

Page 10: In most circumstances it will not be appropriate to use social media to supply information in response to a SAR for information security reasons. Instead you should ask for an alternative delivery address for the response.

If they don't provide an alternative delivery address, then it needs to state the SAR cannot be provided and no further work can take place.

Page 11:- 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.

Does the clock go on hold for this- concerned that to having to look for contact details, get in touch and then wait a response could cut into the timescale for responding

I think they need to be a bit more cautious in terms of what they say you can assume about a person lacking capacity (page 11-12). Under the Mental Capacity Act 2005 it is emphasised that capacity is decision specific. Just because someone may lack capacity to manage their property and financial affairs -which can involve complex decisions- does not mean they lack capacity to make their own SAR-which is simpler- or that you don't need to seek consent/separate authority from the person themselves or at least seek their views (even in the face of a deputyship order or power of attorney) especially if it involves records that dont come within the scope of that power and aren't relevant to its exercise. It would also be helpful to have more guidance on requests from alleged "Litigation Friends" who have not yet been appointed by the Court.

Page 13:- If you have concerns that the individual has not authorised the information to be uploaded to the portal or may not understand what information would be disclosed to the portal, you should contact the individual to make them aware of your concerns.

Again can this be put on hold as we are waiting for clarification?

Page 15:- Can we deal with a request in our normal course of business?

It is important to draw a practical distinction between formal requests for information and routine correspondence that you can deal with in the normal course of business. For example, if an individual requests copies of letters which you have sent to them previously, it is unlikely that you need to deal with this as a formal SAR. You should consider such correspondence on a case by case basis.

Can we have another example of this and when it would apply within the guidance

Page 16:- You should calculate the time limit from the day you receive the request, fee or other requested information (whether it is a working day or not) until the corresponding calendar date in the next month.

Is this request received into the organisation or with the appropriate area for logging/processing the request as depending on the method the query comes in, e.g post, the timescale for this may vary

Page 18:- 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.

Is there anywhere this needs to be documented as part of the response (but not necessarily shared with the requestor?)

Page 18: an individual requests further copies of their data following a request

If you have already provided it as part of a SAR and get the same request can you refuse it on the basis that you have already provided that information

Page 21: If the requested information is not sufficient and you need to take further steps to verify the individual's identity, the timescale for responding begins once you have completed the verification. However, this only applies in exceptional circumstances and generally the timescale for responding to a SAR begins upon receipt of the requested information.

This would need to happen in all occasions.

Page 23:- 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.

If we are waiting for clarification from the requestor- does this point then go on hold?

It's not really clear (page 23) as to whether justifiably asking for additional information to help locate the requested information serves to pause the clock as comment on timescale appears in the next paragraph about a request for all information. I would suggest it would be reasonable, if clarity on this issue is required, to only start the clock when they have responded as how can you begin to deal with it otherwise?

- searching for personal data for a SAR from 'deleted', 'archived' and 'back up' systems. On the one hand the guidance says that information is 'deleted' (p25) when 'you try to permanently discard it and you have no intention of ever using it again'. It then in other paragraphs sets out an expectation that back up should be included in SARs and archived information. I would suggest that it would be easier to apply a distinction that if a "front end user" cannot access the personal data, that this would be sufficient to not include in a search for personal data. Technical expertise is not defined and neither is 'expensive'. The ICO states themselves on **P24** that 'it is very difficult to truly erase all electronic records you may hold data that you do not have ready access to and that requires technical expertise to retrieve.' The guidance,

seems to be stating that an onerous search of back up, archives and deleted information should be searched. This would need to be done in every case as we would not know what had or hadn't been deleted in the instance of emails containing personal data. The guidance then goes onto say that the ICO will not 'seek to take enforcement action against an organisation that has failed to use extreme measures to recreate 'deleted' personal data held in electronic form. We do not require organisation to use time and effort reconstituting information that they have deleted as part of their general records management.' All of this feels quite contradictory and confusing and very onerous.

Page 24:- However, a requester is entitled to ask for 'all the information you hold' about them. If an individual refuses to provide any additional information or does not respond to you, you must still comply with their request by making reasonable searches for the information covered by the request. The time limit is not paused whilst you wait for a response, so you should begin searching for information as soon as possible.

Does this mean that if we are going to them for clarification that a request doesn't go on hold- not quite clear

This needs to be changed to only start the clock once they have clarified, as you could be providing information that they don't want to receive, as well as wasting the time of the organisation to gather the information.

Page 25: 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.

This needs to apply in the case of personal data being in back up tapes.

Page 30:- The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents containing their personal data. You may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out of the relevant information from your computer systems. Although the easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so.

What about when it's not clear what the requestor wants and it might be easier to sit down and show them their record? What about CCTV?

Page 36:-

It would be helpful if the ICO set out what a 'reasonable interval' is in their view with regards to repeated requests and definition of excessive

Page 37:-

The initial reference to exemptions at p.37 is very brief. I think they would do better to point/refer to the pages further on that go into more detail so that the reader would know to look further for more specific guidance on them or to place the third party data section (that talks about "other individuals") before the section on "when can we refuse to comply" rather than after it so that the detail of the exemptions follows after. After all, third party data is not really an exemption or a refusal to comply. This is what the guidance wrongly implies by setting it out in this manner. It just isn't their data so they're not actually entitled to it as

it doesn't fall within the scope of the request/right. It may also be helpful if they were to set out what the Act says in terms of being able to withhold or restrict information under s.45 and how this relates to/ties in with the exemptions i.e. The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

o avoid obstructing an official or legal inquiry, investigation or procedure;

o avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

o protect public security;

o protect national security;

o protect the rights and freedoms of others.

Page 38: If you believe a request is manifestly unfounded or excessive you must be able to demonstrate this to the individual. Where an exemption applies, the reasons you give to an individual for not complying with a request may depend upon the particular case. For example, if telling an individual that you have applied a particular exemption would prejudice the purpose of that exemption, your response may be more general. However, if it is appropriate to do so, you should be transparent about your reasons for withholding information.

It would be beneficial for an example to be given on what to tell the requester is they have put in an SAR but the information is being withheld because e.g. the personal data relates to the prevention or detection of crime, so their personal data cannot be supplied.

Page 51:- Personal data is exempt from the right of access if it is processed for the purposes of discharging a function of:

• the Legal Services Board;

• considering a complaint under: o Part 6 of the Legal Services Act 2007,

o Section 14 of the NHS Redress Act 2006,

o Section 113(1) or (2), or Section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003,

o Section 24D or 26 of the Children's Act 1989, or

o Part 2A of the Public Services Ombudsman (Wales) Act 2005; or

• considering a complaint or representations under Chapter 1, Part 10 of the Social Services and Well-being (Wales) Act 2014.

What about safeguarding information held by all local authorities- is this exempt- and can it be clarified as we often get asked for information in safeguarding reviews/reports