Redaction guidance

1. Introduction

1.1 This note provides guidance to staff that will be preparing and redacting (removing) personal information from documents requested for disclosure under the Data Protection Act 2018 (DPA).

2. Disclosure process

2.1 Always make a copy of the original document (s), and perform any redaction on the copied version.

2.2 Keep three copies, the original, one with redactions marked/highlighted and one fully redacted (with information blacked out/removed)

2.3 The review of the information should be undertaken or checked by an officer with knowledge of the case or relevant subject area.

2.4 Sections 3 to 5 provide guidance on whether or not information should be redacted, further guidance is available from the Council's Information Governance & Risk Team.

2.5 When considering the withholding or disclosure of information, remember that you have an obligation to communicate as much of the information requested as you can without disclosing the identity of any third party or exempt information.

2.6 A copy of the information disclosed to the data subject should be added to the client's file, along with an explanation as to why any information has been redacted. Where third party information is disclosed, the reasons for disclosure should also be recorded.

2.7 Under the DPA we must respond to a Subject Access Request in no longer than 30 calendar days (although we can extend legally in some cases).

2.8 Where the information being provided to the data subject could cause them distress or harm, you should consider whether it would be prudent to meet with them to discuss and explain the information being provided. Section 5.1 of this guidance covers prejudice to mental or physical health, and may assist in identifying the circumstances when a meeting may be appropriate.

2.9 **Redacting physical documents**

2.9.1 Redactions can be made to physical documents using redaction tape or a black marker pen. Alternatively the document can be scanned and edited electronically.

2.9.2 After all the information has been redacted from the physical document, it must be scanned and checked to ensure all the redacted information is unreadable.

2.9.3 A copy of the marked and redacted copies should be provided to Information Governance & Risk for disclosure to the requester.

2.9.4 Copies of all documents should be retained on the requesters personal or similar Council system file.

2.10 **Redacting electronic documents**

2.10.1 Redactions to electronic documents should be made using the latest version of Adobe Writer (This can be obtained from Corporate ICT).

2.10.2 Do not redact Word documents, as redactions made to these can (in some circumstances) be reversed and made visible again.

2.10.3 Following redaction, electronic documents should be saved to PDF for disclosure.

2.10.4 A copy of the marked and redacted copies should be provided to Information Governance & Risk for disclosure to the requester.

2.10.5 Copies of all documents should be retained on the requesters personal/LiquidLogic or similar system file.

3. Information already known by the data subject

3.1 The following Information would normally be provided to the data subject

a) Information originally provided by them;

b) Information previously provided to them, except where information was provided to them in error;

c) Information already known by them;

d) Information generally available to the public.

3.2 Information likely to be known by the individual making the request;

3.2.1 Some information is likely to be already known by the individual making the request, for example third party information relating to a member of staff (acting in the course of their professional 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.

4 Third party information

4.1 It is very likely that a case file for a data subject will include personal information about other individuals, who have been involved in or affected by their case. In some cases, particularly older cases, case files could be a joint or family record.

4.2 Every effort should be made to contact any third party, to ascertain if they consent to the disclosure of their personal information. In contacting the third party you must ensure the privacy of the data subject is also maintained. The consent or refusal of the third party must be recorded.

4.3 Where you do not have the consent of the third party, you must consider whether it would be reasonable in all circumstances to disclose the information relating to the third party without their consent. The considerations when deciding whether it would be 'reasonable in all circumstances' to disclose third party information is as follows:

a) any duty of confidentiality owed to the other individual, .
b) any steps taken by the data controller with a view to seeking the consent of the other individual, .
c) whether the other individual is capable of giving consent, and.
d) any express refusal of consent by the other individual

4.4 If you have not got the consent of the third party and you are not satisfied that it would be reasonable in all the circumstances to disclose the third party information then you should withhold it. However, you are obliged to communicate as much of the information requested as you can without disclosing the identity of the third party. So, disclosing the information with any third party information edited or deleted may be the best way to comply with the request if you cannot disclose all the information.

4.5 When making your final decision about what information about third parties should be disclosed, you should review all the matters you have considered and all of the efforts you have made to get consent. The reasons for your decision on whether or not to disclose must be recorded on the case record.

4.6 **Information about relatives**

4.6.1 We need to distinguish between a relative's personal information (withhold) and information about that relative that is also information about the person making the request (disclose).

For example "The child was voluntarily accommodated as mum was unable to cope due to post natal depression"

Could be edited as follows: "The child was voluntarily accommodated [redacted]"

or "The child was voluntarily accommodated as mum was unable to cope [redacted]"

4.6.2 In balancing the data subject's right to know with Mum's right to privacy, disclosing in line with the second option provides a context that would probably have been shared through life story work without disclosing Mum's mental health issues.

4.7 **Information about Foster Carers**

4.7.1 Again we need to distinguish between factual information provided by Carers in their role as agents for the Authority and personal opinions and/or information they would provide in the same way that a relative might;

For example "Last night the young person returned home drunk [redacted]"

Could be edited as follows, to remove the personal view of the foster carer as

to how they felt: "Last night the young person returned home drunk which felt like a slap in the face"

4.7.2 If the foster carer subsequently told the young person how they felt, the subsequent statement would be released

"I told <name of child to be added> that it felt like a slap in the face".

4.8 **Names of professionals / staff**

4.8.1 The Information Commissioner's advice is that staff names are disclosed provided there is no risk of harm to the staff member involved. The names of the staff that have provided direct services to the person will usually already be known to the data subject.

4.9 **Third Party Opinion**

4.9.1 If an external professional is stating facts that the data subject has already been told (e.g. within a multi-agency meeting where the client was involved in the discussion) they can be disclosed;

4.9.2 However, where a third party is giving an opinion then this would not normally be disclosed without their or their organisation's consent.

4.9.3 Even so, where we do not have consent we still need to consider whether it would be reasonable to release the third party information, as the opinion may have affected how the data subject was treated.

4.10 **Confidentiality**

4.10.1 Another factor to be considered in assessing how reasonable a disclosure would be is whether a duty of confidence exists for the third party information.

4.10.2 This would arise where information which is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to you with the expectation that it will remain confidential. This expectation might result from the relationship between the parties. For instance, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

a) Medical (doctor/patient);

b) Employment (employer/employee);
c) Legal (solicitor/client);
d) Financial (bank/customer);
e) Caring (counsellor/client).

4.10.3 However, you should not always assume confidentiality. For instance, just because a letter is marked 'confidential', a duty of confidence does not necessarily arise (although this marking may indicate an expectation of confidence).

4.10.4 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.

4.10.5 However, in most cases where a clear duty of confidence does exist, it will usually be reasonable to withhold third party information unless you have the consent of the third party individual to disclose it.

5 Other considerations

5.1 Prejudice to mental or physical health

5.1.1 Where disclosure of information would result in harm to the person or another individual, the opinion of a relevant medical professional must be sought on the possibility of harm as a result of disclosure. There must however be a quantifiable likelihood of serious harm to a person before an exemption can be applied.

5.1.2 When obtaining the views of a relevant medical professional, you must ensure the privacy of the data subject is maintained.

5.2 Crime related information

5.2.1 Information can be withheld if its disclosure would actually prejudice the prevention or detection of a crime or the apprehension or prosecution of offenders.

5.3 Legal Professional Privilege

5.3.1 Discussions with and advice from our legal department or from Counsel instructed on behalf of the Council may be exempt from disclosure on the

basis of legal professional privilege.

5.3.2 Any legal information must be reviewed by our legal services department to determine whether or not it can be disclosed.

5.4 **Court documents**

5.4.1 Any Court documents must be reviewed by our legal department to determine whether or not it can be disclosed.

5.5 **Self Incrimination**

5.5.1 If the case file you are redacting includes information which would reveal evidence of an offence and thereby expose the Council to criminal proceedings, your Head of Service and Information Governance & Risk, plus The Council's Legal Services department must be informed immediately.

6. Further information

6.1 For Advice and further guidance, please contact the Council's Information Governance & Risk team at:

Info.requests@leicester.gov.uk