Redaction Guidance for Disclosure Team

Identifying and applying redaction correctly is a very important check. This must be done diligently to ensure that confidential data is not accidentally disclosed unintentionally.

Principals of redactions

What are we disclosing

- Subject Access Request bundles under the Data Protection Act, or
- Responses to Information requests under Freedom of Information Act or Environmental Information Regulations
- Court Orders

How are we disclosing – safe and secure

- Redaction is the separation of disclosable from non-disclosable information by the blocking out, removal or substituting of individual words, sentences, paragraphs, pages or sections prior to its release or publication.
- Most information request under the Data Protection Act, Freedom of Information Act and Environmental Information Regulations will contain a mixture of information that can be disclosed and information that is subject to an exemption or exception.
- Under the legislation there is an obligation to communicate as much of the requested information as possible. Therefore, blanket exemptions or exceptions to a whole document from disclosure will not normally apply or be lawful; you can only withhold the whole document or data set when all the information is exempt or excepted from disclosure. 3.4 Redaction is normally carried out to remove words, sentences or paragraphs, but if so much information has to be redacted that a document becomes unreadable it may be appropriate to withhold individual sections, pages or even the entire document.
- Be clear on what data falls within the scope of the request you are dealing with, just because you have access to information does not mean you are authorised to disclose that information or that it falls within the scope of the request.

Redactions should be applied on a case by case basis and the the Trust as a Data Controller will consider whether disclosing this information is necessary; likely to cause harm; likely to prejudice; and reasonable in all the circumstances. As a matter of good practice, a copy of the disclosure bundle showing the redactions and the reasons behind them should be retained for reference.

Examples of this include:

a) Information you hold on behalf of another organisation or third party;
b) Information you have access to through a shared system.

If any of the above scenarios are applicable then the requester should be sign posted to the relevant organisation or third party for the information.

- The following principles must be followed when reviewing information or documents prior to disclosure or publication:

a) The review should be undertaken by someone with a detailed knowledge of the case or relevant subject area;
b) Never redact the original source information or document. Always make a copy and perform the redaction on the copied version;
    - If printing or photocopying information for redaction, this must be single sided – to prevent redactions showing through on the reverse side.
c) Consider whether any other factors are important for the understanding of the information e.g.
    - Does colour provide meaning; or
    - Is a key or an explanation of abbreviations needed.
d) Always use the most effective redaction method available, and consider the limitations of that chosen method
e) When reviewing information for disclosure, as well as checking the content of the document or data set, checks must also be undertaken of the File Properties / Meta data (section 8) and for 'hidden content (section 9);
f) After the redaction process has been completed a new copy of the information should be created and thoroughly checked to ensure all the redacted information has been **removed** or is **unreadable** and the redaction process **cannot be reversed**;
g) All intermediate copies of the information created during the redaction process and any waste must be securely destroyed;
h) Two copies of the disclosed information should be made
    - One will be retained as an evidential record of the disclosure, along with an explanation as to why any information has been redacted, or disclosed for example in the case of third party personal data;
    - The second copy is for the requester. Normally the copy will be provided to them in an electronic format, unless they have specified otherwise.
i) If there are any concerns that disclosing the information may cause harm or distress to the recipient, consideration should be given to offering them advice or assistance including a meeting as part of the disclosure process.

Information that may be exempt from disclosure

Below are examples of the information, which may be exempt from disclosure:

- Personal identifiable data
- could cause prejudice to the health or the delivery of social care services of a service user.
- could jeopardise the safety of any individual;
- would prejudice the prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of tax;
- a claim to legal professional privilege can be maintained;
- Court documents in specified circumstances;
- a prohibition or restriction from disclosure applies;
- would, or would be likely to, prejudice commercial interests of any person or legal entity;
- in relation to negotiations, if would be likely to prejudice those negotiations
- in relation to management forecasting or planning, if would prejudice the conduct of the business or activity concerned;
- Confidential references; and
- provided with an expectation of confidentiality * e.g. complaints, safeguarding concerns, whistleblowing or fraud referrals.

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. 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.

- Exemptions must be considered on a case-by-case basis, and are open to appeal by the individual making a request, so it is important to document the reasons which informed your decision.
- Further details on what information could potentially be exempt from disclosure, is available through the:
    - Data Protection Act 2018 / UK GDPR
    - Freedom of Information Act;
    - Environmental Information Regulations;
    - ICO's website;
- Information already known by an individual: Whilst information or documents originally provided by or given to an individual would normally be disclosed, it is important to consider if they still have a justified purpose for receiving the information: a)
    - If information is about a third party, do they still have an involvement / relationship with that individual that justifies disclosure;
    - If information was provided to them in relation to a specific role / duty they were undertaking at the time does that justified basis still apply;
    - Was the information previously provided to them in error;
    - Have any other circumstances changed since the original provision or disclosure of the information?

Requests on behalf of children & young people:

Parents or guardian may make requests for information about children and young people. It is important to remember that whilst the parent or guardian may be making the request, the right of access is that of the child or young person and the request is being made on their behalf.

Before responding to a request, you must consider whether the young person is mature enough to understand their rights. If you are confident that the young person can understand their rights, then you should seek their views or authorisation for disclosure

The best interests of the child or young person must considered be at all times.

Exemptions under Data Protection Act

Third party information

Case notes for a data subject will/may include personal data about other individuals, who have been involved in or affected by their case. In some cases, particularly where there are siblings, case notes could be a joint or overlapped.

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 the Trust must ensure the privacy of the data subject is also maintained. The consent or refusal of the third party must be recorded.

Where the Trust does not have the consent of the third party, the Trust 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 Trust 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

If the Trust has not obtained the consent of the third party and the Trust is not satisfied that it would be reasonable in all the circumstances to disclose the third-party information, then this will be withheld / redaction applied.

However, it is imperative to note that the Trust has an obligation to communicate as much information requested, without disclosing the identity of the third party. The disclosure bundle must have any third-party information edited /deleted/redacted with the appropriate redaction method to comply with the request if the Trust cannot disclose all the information.

The reasons for your decision on whether or not to disclose should be ideally recorded on the case management system.

Information about relatives

When applying an exemption, the Trust will need to distinguish between a relative's personal data (withhold) and information about that relative that is also information about the person making the request (disclose).

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.

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]"

Information about Foster Carers

Personal data about foster carers ca sometimes be on the case notes. Where there is a safeguarding risk or a risk of harm on the placed child, the details of the foster carer MUST not be included in the disclosure bundle.

Factual information provided by Carers in their role as agents for the Trust and personal opinions and/or information they would provide in the same way that a relative might.

Names of professionals / staff

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.

Third Party Opinion

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.

Metadata and Hidden Information

Whenever you create a file (e.g. word document, spreadsheet, presentation or email) or folder, Windows automatically collects information about it including the author and a version history. To see the file properties right-click the item in the folder and choose Properties from the pop-up menu.

'Hidden' information in documents.

Most data or information within a document or dataset will be clearly visible or identifiable however, the following examples illustrate when this may not be the case:

a) Hidden by formatting styles: The author when creating a template may have chosen to 'hide' certain data by setting the font colour to be the same as the background (e.g. white on white or black on black). Whilst this would prevent disclosure if printed, it would remain accessible within a digital copy;
b) Layered content: where pictures or objects have been overlaid or placed over other content;
c) Placed outside the area of display: The author may have placed data at the end or edge of the document which is outside the normal visible area e.g. EXCEL has supports over 16 thousand columns and 1 million rows of data;
d) Hidden rows and columns: EXCEL includes a function to 'hide' rows or columns from view, which can then be 'unhide'. This can be identified as rows or columns will not run consecutively;
e) Hidden worksheets: EXCEL also allows an entire worksheet to be hidden from view;
f) Embedded documents or files: Files and document can be inserted or pasted into documents;
g) Pivot tables: The source data summarised within a Pivot table can be retrieved by double-clicking on the table, even if the original worksheet has been deleted or the Pivot table has been copied into a new workbook;
h) Charts: Charts like Pivot tables can contain an embedded copy of the source data within them;
i) Functions: Functions such as LOOKUP and VLOOKUP also create and store a cache of the source data which can potentially be retrieved even if copied into a new workbook or document; and
j) The 'Track Changes' feature in WORD: This can be turned on through the Review tab, and marks up and shows any changes that anyone makes to the document i.e. deleted text is retained within the document but displayed as struck through until approved or rejected. This feature allows you to see the document in its original version or the intended final version. It is therefore possible for you to receive a document without realising that 'Track Changes' has been turned on, which contains hidden comments or changes that have not been approved or rejected.

The ICO's How to disclose information safely: Removing personal data from information requests and datasets, which provides more in-depth examples on potential unintended disclosures and how to identify and remove them;

The National Archives Redaction Toolkit, which provides guidance on editing exempt information from paper and electronic documents.