Review date: May 2021

Redaction Guidance
(Disclosing Information Safely)

1. Introduction

1.1 In the course of our activities, we are required to disclose or publish information.

a) In response to general enquiries, a Subject Access Request under the Data Protection Act, or information requests under Freedom of Information Act or Environmental Information Regulations;
b) As part of papers supporting activities (e.g. Court papers) or meetings (e.g. Committees);
c) To comply with a statutory duty (e.g. Court Order, Transparency Code);
d) As part of media or promotional activities;
e) As part of research or within case studies; or
f) In making data available for re-use under the Reuse of Public Sector Information Regulations.

1.2 Before disclosing or publishing information, it is important to check that it does not include any information either exempt from disclosure or not intended for publication.

a) Personal identifiable information other than that which is the personal data of an individual making a SAR request;
b) Data that would jeopardise the safety of any individual or group;
c) Data that would jeopardise the prevention or detection of crime, the apprehension or prosecution of offenders or the collection of taxes;
d) Data in relation to negotiations, which would prejudice those negotiations;
e) Data that would, or would be likely to, prejudice commercial interests;
f) Data covered by legal professional privilege; and
g) Data which would prejudice management forecasting or planning

1.3 Failure to do this could result in a data breach with privacy or safety implications for individuals; commercial implications; complaints; reputational damage; enforcement action and / or financial penalties.

1.4 This guidance supports our Records Management Policy, Data Protection Policy, Access to Information Policy and ICT and Information Security Policy and provides advice on the creation, review, redaction and appropriate disclosure of information.

1.5 Information may not always be easily visible within documents or data sets, and this guidance identifies common examples of information can be 'hidden' from view.

2. Privacy by Design and Default

2.1 Privacy by design and default is an approach that ensures privacy and data protection issues are considered at the design phase of any system, service, product or process and continue throughout it's lifecycle, by

a) putting in place appropriate technical and organisational measures designed to implement the data protection principles; and
b) integrating safeguards into the processing to meet data protection requirements and protect the rights of individuals.

2.2 Following an approach of privacy by design and default and having an expectation that the information you collect will be at some time in the future be asked for by a third party, will enable you anticipate, avoid and reduce the need for the redaction of information prior to disclosure.

2.3 Examples of privacy by design and default which can reduce the need for redaction include:

a) Data minimisation: only collecting the minimum amount of information relevant and necessary for your purpose;
b) De-identifying information: considering if information needs to be used at an identifiable level, or could the same result be achieved with aggregated, anonymised or pseudonymised information. Even if identifiable information is needed initially, information should be de-identified as soon as possible;
c) Retention: only keeping the information for as long as is necessary;
d) Transparency: clearly informing individuals how their information will be used, including when, how and who their information may be disclosed to through Privacy Notices;
e) In process, template and form design, looking to avoid duplication / repetition of information e.g. in a template consider detailing the personal data of the individual in a separate section, which is then referenced within the content rather than repeated;
f) Data Protection Impact Assessments, which help to reduce potential risks.

2.4 For more details about on Data Protection by Design and Default visit the ICO's website.

3. Redaction principles

3.1 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.

3.2 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.

3.3 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.

3.5 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. 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.

3.6 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 (see Appendices 1 & 2);

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

   a. 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;

   b. 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.

4. Information that may be exempt from disclosure

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

a) Personal identifiable data (see sections 5, 6 & 7 for further details);
b) could cause prejudice to the health of any individual in the opinion of a relevant medical professional;
c) could jeopardise the safety of any individual;
d) would prejudice the prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of tax;
e) a claim to legal professional privilege can be maintained;
f) Court documents in specified circumstances;
g) a prohibition or restriction from disclosure applies;
h) would, or would be likely to, prejudice commercial interests of any person or legal entity;
i) in relation to negotiations, if would be likely to prejudice those negotiations;
j) in relation to management forecasting or planning, if would prejudice the conduct of the business or activity concerned;
k) Confidential references; and
l) 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.

4.2 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.

4.3 Further details on what information could potentially be exempt from disclosure, is available through the:

a) Data Protection Act 2018 / General Data Protection Regulation;
b) Freedom of Information Act;
c) Environmental Information Regulations;
d) ICO's website; and
e) For NEL CCG and Council staff the Data Protection Officer transparency@nelincs.gov.uk

4.4 **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;
b) 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;
c) Was the information previously provided to them in error;
d) Have any other circumstances changed since the original provision or disclosure of the information?

5. Requests on behalf of children & young people:

5.1 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.

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

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

6. Personal data

6.1 'Personal data' is defined in the General Data Protection Regulation as meaning any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

6.2 Other examples of identifiers include:

Initials; Job titles or roles; Gender references (in certain circumstances); Reference numbers (e.g. NINO, NHS No., claim); Telephone numbers; Email addresses; Descriptions; and Signatures.

6.3 Remember that combinations of information, whilst not personal data in isolation, when brought together could result in the identification of an individual.

7. Right of Access and personal data of others

7.1 The Data Protection Act 2018 gives an individual a right of access to the personal data held about them. It is very likely that an individual's file or record will include information about or referencing other individuals, who have been involved in or affected by the case. In some cases, particularly older cases, case files and records could be a joint or family record.

7.2 Schedule 2 Part 3 paragraph 16 (Protection of the rights of others: general) of the **Data Protection Act 2018** states:

1) Article 15 (1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.
2) Sub-paragraph (1) does not remove the controller's obligation where—

   (a) the other individual has consented to the disclosure of the information to the data subject, or

   (b) it is reasonable to disclose the information to the data subject without the consent of the other individual.
3) In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—

(a) the type of information that would be disclosed,

(b) any duty of confidentiality owed to the other individual,

(c) any steps taken by the controller with a view to seeking the consent of the other individual,

(d) whether the other individual is capable of giving consent, and

(e) any express refusal of consent by the other individual.

4) For the purposes of this paragraph—

(a) "information relating to another individual" includes information identifying the other individual as the source of information;

(b) an individual can be identified from information to be provided to a data subject by a controller if the individual can be identified from—

(i) that information, or

(ii) that information and any other information that the controller reasonably believes the data subject is likely to possess or obtain.

7.3 Always consider the privacy and rights of all the individuals involved before contacting any third party.

7.4 The reasons for your decision on whether or not to disclose the personal data of another individual must be documented including the efforts you have made to seek consent.

7.5 When determining whether it is reasonable to disclose the information without consent, consideration must be given to the context of the information and whether the information is actually personal data and who the personal data actually relates to:

a) The names of professionals, which have provided services directly to an individual, will usually already be known to them, and the ICO's advice is that their names are disclosed provided there is no risk of harm to them.

7.6 The ICO's guidance 'Access to information held in complaint files' provides further guidance about the disclosure of personal data.

8. File properties / Meta data

8.1 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.

8.2 To see the file properties right-click the item in the folder and choose Properties from the pop-up menu.

9. 'Hidden' information in documents

9.1 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

also 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.

9.2 Further guidance can be found in:

- 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.

10. General rules to avoid 'hidden' information

10.1 **Never use** a previous document as a template for your new document, as it will contain data or references to the original subject - **Always** use the agreed blank template.

10.2 **Apply consistent formatting throughout the document.** Use consistent font and background colours and shading to avoid black on black or white on white situations occurring. Please note that the automatic font colour is preferable to using black, as automatic will ensure text is visible when a dark shading is applied.

10.3 **Only include information that is necessary**

a) When possible provide information at a summarised, anonymised or pseudonymised level rather than at a detailed or identifiable level.

10.4 **Consider the source data in Pivot Tables and Charts and if possible use the Paste as 'value only' option** to remove the link to the source data.

10.5 **When pasting large quantities of data into table cells** consider if there are size restrictions, which will mean not all of the data will be visible.

10.6 **Do not hide data within the document.**

a) Consider creating alternative versions if different levels of access are required;
b) Consider the potential consequences before
   i. Placing data outside of the main viewing / content area;
   ii. Overlaying objects;
   iii. Hiding rows, columns or worksheets;
   iv. Embedding documents or files;
   v. Including hyperlinks.

10.7 **If there is a requirement to hide information in a document** then record the type of information hidden and its location within the document to prevent the risk of it being missed and to assist with future redaction.

10.8 **Delete cropped areas of pictures.**

10.9 **Check if the 'Track Changes' feature is turned on and if Mark ups are visible**

10.10 **General considerations for the creation of documents** include:

a) Using file and folder names than do not include non-disclosable information;
b) Set print areas;
c) In Excel delete unused sheets.

Appendix 1 – Redaction methods for Physical Documents

Blocking out	Using redaction tape or a redaction pen. A normal biro or marker pen **must not** be used for redaction as this can leave information still visible after blocking out. This method can allow the size of the removed text to be determined, potentially assisting in the identification of the original information.
Removal	Cutting out with a scalpel or scissors. The removed parts of the document must then be cross-cut shredded. This method can allow the size of the removed text to be determined, potentially assisting in the identification of the original information.
Substituting	Providing a summarised version of the document using aggregated or anonymised terms in place of the removed text as appropriate e.g. Complainant, Officer 1, Landlord, etc. It is **not recommended** to replace text with xxx's as this can identify the number of letters in a word or name, potentially assisting in the identification of the original information.

Appendix 2 – Redaction methods for Electronic Documents

a) **ALWAYS USE** the Document Inspector function to review your document and identify, approve or remove, Comments, Revisions, Versions and Annotations; Document Properties and Personal Information; Custom XML data; Headers, Footers and Watermarks; Invisible Content; and Hidden Text.

Blocking out Removal	Using a redaction / annotation tool to remove the text and either leaving it blank or replacing it with coloured boxes. Changing the font colour of the text to the colour of the background to hide it, **must not** be used as it can be easily reserved
Substituting	Providing a summarised version of the document using aggregated or anonymised information as appropriate e.g. Complainant, Officer 1 etc, Landlord; or Using a redaction / annotation tool to remove the text and replacing it with 'Text Redacted' It is **not recommended** to replace text with 'xxx' as this can identify the number of letters in a word or name, potentially assisting in the identification of the original information. To assist with the understanding of the information, text can be replaced by a description e.g. Complainant, Officer 1 etc, Landlord.

b) Redaction of electronic documents in Legal Services were possible must be undertaken using RapidRedact.

Appendix 3 – Electronic Document Redaction Checklist

The following checklist is adapted from the ICO's guidance and highlights a number of things to consider when reviewing different types of document.

Document types	Check
General - All documents Email Images/Video PDF Presentations Spreadsheets Word	○ Document title or filename for non-disclosable information (e.g. names, locations) ○ File properties / versions for non-disclosable information ○ Comments for non-disclosable information ○ Headers and Footers for non-disclosable information ○ That font and background colours are not set to the same colour in order to hide information ○ For content under / overlaid by other objects ○ For embedded / attached documents or data ○ For Macros / Custom XML data ○ Pivot tables and charts for linked data ○ For hidden hyperlinks ○ If the file size is larger than you might expect for the volume of data being disclosed ○ All redactions are effectively applied
Email	○ All correspondence including hyperlinks and attachments in the email chain
Images/Video	○ If images contain non-disclosable information (e.g. faces of third-party individuals, contents of whiteboards or notice boards)
Presentations	○ Presenter notes for non-disclosable information ○ For hidden transitions or slides
Spreadsheets	○ For hidden columns, rows or work sheets ○ For Filters ○ For Defined Scenarios ○ You know where all the data is? The Ctrl+End command goes to the last cell used on the current sheet ○ If formulas link to external files ○ Truncated / non-wrapped content in cells or tables
Word	○ Watermarks ○ TRACK CHANGES is set to All Markup / Final: Show Markup and changes are viewable ○ All changes have been 'Approved' or 'Rejected'