APPENDIX 2

Redaction Guidance

Date: December 2021

Version: V1.0

APPENDIX 2

Document Version Control

Document Version Control		
Version	**Date**	**Approved by**
1.0	November 2021	Information Governance Group – 2 December 2021
1.0	March 2022	Audit Panel – 15 March 2022

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. INTRODUCTION

1.1. In the course of its activities, Tameside Metropolitan Borough Council ("The Council") is required to disclose or publish information:

- In response to general enquiries, a Subject Access Request under the Data Protection Act 2018 ("DPA 2018"), or information requests under the Freedom of Information Act 2000 ("FOIA 2000") or Environmental Information Regulations 2004 ("EIR 2004");
- As part of papers supporting activities (e.g. Court papers) or meetings (e.g. Committees);
- To comply with a statutory duty (e.g. Court Order, Local Government Transparency Code);
- As part of media or promotional activities;
- As part of research or within case studies; or
- 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 that is exempt from disclosure or not intended for publication, such as:

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

1.3. Disclosure of such information could result in a data breach with privacy or safety implications for the individuals concerned, commercial implications, complaints, reputational damage, enforcement action and/or financial penalties.

2. DEFINITIONS

2.1. The following terms are used throughout this document and are defined as follows:

Table 1 – Definitions

Term	Definition
Personal Data	Is any personal data as defined by UK GDPR and the Data Protection Act 2018. It is defined in the Data Protection Act 2018 at **s.3(2)** as "any information relating to an identified or identifiable living individual." Broadly, this means any information (relating to a living individual who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council. The UK GDPR provides a non-exhaustive list of identifiers, including:

Term	Definition
	• Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person. The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.
Special Category Data	This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of: • Racial or ethnic origin • political opinions / beliefs • religious or philosophical beliefs • trade union membership • genetic data • biometric data (where used for ID purposes) • health; • sex life; or • sexual orientation. Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.
Confidential information	Is any information has the necessary quality of confidence (which means that it is not generally available to the public and is not trivial) and is imparted in circumstances whereby the party making the disclosure has a reasonable expectation that the information will remain confidential.
Protected Information	Is any information which is: • Personal / Special Category Data; or Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.
Employee(s)	Includes all employees, Members of the Council, Committees, temporary staff, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes Including:- • Customers • Current, past and prospective employees • Contractors

Term	Definition
	• Councillors • Suppliers • Service Users • Carers (including Foster Carers) • Residents • Others with whom the Council communicates.

3. SCOPE OF THIS GUIDANCE

3.1. This guidance has been drawn up to provide clear guidance on the Council's approach to redaction and ensure a consistent, standardised approach by all employees to protecting personal and confidential information. A failure to follow this guidance may result in disciplinary action.

3.2. This guidance applies to all employees and should be read in conjunction with the Council's other related documents, in particular the Subject Access Request Guidance, found on the Council's Data Protection/Information Governance Intranet page.

3.3. This guidance will be reviewed annually to make sure it reflects changes in the organisation, data protection legislation and taking into account guidance from the Information Commissioners Office (ICO).

4. ROLES AND RESPONSIBILITIES

4.1. Employees

4.1.1. All employees responsible for publishing and disclosing data/information and documents must be aware of the types and categories of data/information and the circumstances that require redaction. Employees must follow the guidance set out in this document and other Data Protect/Information Governance Framework documents in order to ensure that data/information is redacted appropriately and irreversibly where required.

4.1.2. Employees must use the redaction software authorised and provided by IT services. Use of any other method of redaction (black marker, highlighting text in black in Microsoft Word / Adobe Acrobat Reader) is strictly prohibited as the redaction may not fully obliterate the text beneath it, or could even be fully reversed.

4.2. Managers

4.2.1. All managers are responsible for being aware of the Redaction Guidance and ensuring compliance by their team members.

4.2.2. Where team members have responsibility for redaction, managers are responsible for ensuring that the team member has access to and full use of the redaction software authorised and provided by IT services. For the avoidance of doubt, redaction may only be undertaken using the approved software and managers must not allow any redaction to take place by an employee until they have access to the software.

4.2.3. Managers are also responsible for double checking any redaction undertaken before the data/information is published or disclosed, notifying the Directorate IG Champions with issues and seeking advice and assistance where needed.

4.3. Heads of Service

4.3.1. Heads of Service are assigned responsibility for the main systems and information assets within their business area. The Head of Service is responsible for monitoring compliance with the UK GDPR and the DPA 2018 in respect of the information they 'own', which includes compliance with protection of personal and confidential data/information. They are responsible for selecting appropriate employees within their Service to be responsible for dealing with redaction tasks and identifying different senior employees within their Service to act as Directorate IG Champions. In the event of a complaint about the way redaction has been applied, the Head of Service is responsible for ensuring the complaint is properly investigated and approving the response.

4.4. Directorate IG Champions

4.4.1. Directorate IG Champions have been appointed within Directorates to provide advice and support in relation to data protection/information.

4.5. IT Services

4.6. IT Services will provide appropriate systems, software and guidance to any employee with responsibility for carrying out redaction. Where new employees require access to the redaction software, IT Services will, on request, arrange to set up access to this software and provide appropriate training materials to any new user. IT Services will to publish user guides for the software on the service desk and will ensure any updated guides provided by the software publisher are rolled out in a timely manner. The current redaction software is PDF Studio, and the user guide can be found on the IT service desk on the Intranet.

5. WHAT IS REDACTION?

5.1. Redaction is a process which is undertaken to render data/information unreadable. There may be different reasons why data/information should be withheld, but one common reason for redacting documents and files is to ensure information about others is not disclosed inappropriately when sending out responses to requests for data/information.

5.2. Redaction is done by blocking out individual words, sentences or paragraphs or by removing whole pages or sections prior to the release of the document. Redactions should not just be blank space, it should be clear that redactions have been made to a document and the amount of information redacted should also be clear.

6. REDACTION PRINCIPLES

6.1. Redaction must never be undertaken on an original document. Employees must always make a copy of the original document(s), and perform the redaction on the copied version. The copy document must be saved as the same name as the original document with the word 'redacted' inserted in the title. Failure to follow this naming convention correctly on the original and redacted documents may result in accidental disclosure of the unredacted version, which could cause a data breach and may lead to disciplinary action.

6.2. The original document(s) will be retained (either in hard copy or electronic format) for the appropriate retention period as set out in the Retention and Disposal Guidance and Schedule.

6.3. When dealing with requests that involve hard copy/paper records, those records must be scanned into the Council's system to be redacted electronically.

6.4. Redactions should be made using the software approved and supplied by IT Services, currently PDF Studio. Redactions on Microsoft Word and Adobe are not appropriate as they can be undone by the recipient. A user guide for the redaction software can be found on the IT Helpdesk by searching for “redaction”.

6.5. Within the current redaction software provided, it is not sufficient simply to use the redaction tool (under the Document Tab on PDF Studio) to highlight text to be redacted and then save it. You must then ‘apply’ the redactions and follow this up by ‘sanitising’ the document to remove any hidden data/metadata/comments/layers in the document. The sanitise function is accessed under Secure Tab>Sanitise on PDF Studio. Once the redactions are applied and sanitised, the document must be ‘flattened’ (under the Document Tab on PDF Studio) which prevents the redactions being undone. Failure to follow this process in full can lead to the redaction being left in a reversible state, or hidden data being accessible to the recipient.

6.6. Only the original version of the document(s)/data/information and the fully redacted version should be retained. Employees should not save a copy of the document with the redaction marks visible but reversible ‘just in case’ as this creates an increased risk that the wrong version of the document is disclosed or published. If the recipient queries or challenges the level of redaction carried out, comparison can be made between the original document (completely unredacted) and the redacted copy document and if necessary, the challenged sections can be redacted again and redisclosed or republished.

6.7. The redacted document/data/information should be converted into a pdf format (using the redaction software) prior to publication or disclosure to prevent carryover of any tracked changes which may allow reversal of the redaction and to prevent unauthorised alteration of the end document by the recipient.

6.8. When redacting data/information from electronic files/documents, you must ensure that there is no hidden data within the file document (e.g. hidden columns/rows or even worksheets on an Excel spreadsheet, white coloured text on a Word document, embedded documents or files within another document etc.). However, conversion to a pdf document, as per 6.7 above, may not completely remove hidden data, which could then be copied and pasted back into a Word Document to enable it to be seen. Care must be taken to ensure that all data (including hidden data) is checked and redacted (or removed if appropriate) before the data/information is published and disclosed.

6.9. When considering the withholding or disclosure of information under UK GDPR, DPA 2018, FOIA 2000 and EIR 2004 there is an obligation to communicate as much of the requested information as possible. As a result, blanket exemptions or exceptions to a whole document being disclosed/published will not normally apply or be lawful. The council can only withhold the whole document or data set when all the data/information contained within is exempt or excepted from disclosure or publication.

6.10. 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. However, if a document needs to be so heavily redacted, but there is information that is relevant and still makes sense after redaction, it may be more appropriate to type the unredacted information out separately or reference it in the response to the disclosure request or at the outset of publication of the data/information.

6.11. A whole sentence or paragraph should not be redacted if only one or two words are non-disclosable, unless release would place the missing words in context and make their content or meaning clear, or allow an individual to be identified either from the context of the sentence or in conjunction with wider information available elsewhere in the disclosure document(s).

6.12. It is important that redactions made to any data/information are consistent and logical, so that if a word is redacted in one part of the document for one reason, if that reason could apply to other text, redactions are also made to the other text based on that same reasoning.

6.13. 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:

- Information you hold on behalf of another organisation or third party;
- 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.

6.14. After all the information has been redacted from the physical document, it must be checked to ensure all the redacted information is unreadable and that the redaction cannot be undone.

6.15. The following information does not normally require redaction:

- Information originally provided by the requester, or parties in legal proceedings;
- Information previously provided to the requester/parties, except where information was provided to them in error;
- Information already known by the requester/parties;
- Information generally available to the public.

6.16. Where you are disclosing data/information in response to a request it is best practice to confirm whether data/information has been redacted and why.

6.17. Above all, if you are in any doubt about whether information should be redacted, seek advice from your directorate IG Champion, the Information and Improvement Team (where in relation to a SAR, FOI or EIR request), the Information Governance Team or Legal Services.