OUTCOME DETAILS

Supreme Court - Civil
at Supreme Court Sydney
on 22 July 2019

2018/00371447-001 / Summons: Richmond Valley Council v JARDINE LLOYD THOMPSON PTY LTD
I make orders in the document entitled Consent Order which I have initialled, dated today's date and placed with the papers.

Consent Order

Terms of Order made by the Court by Consent

1. The parties are to comply with the Electronic Exchange Protocol appearing at Annexure A to these orders for the purpose of giving disclosure in the proceeding.

Justice D Hammerschlag

Signed

Date

ANNEXURE A

PROTOCOL FOR ELECTRONIC EXCHANGE OF DOCUMENTS

In the Supreme Court of NSW

Equity Division

Proceeding No. 2018/00371447

BETWEEN

Richmond Valley Council, *Plaintiff*

AND

Jardine Lloyd Thompson Pty Ltd, *Defendant*

1. Purpose of this Document

The purpose of this document is to provide a protocol for the electronic exchange of data and images for both hardcopy and electronic documents. This will ensure that all parties are able to view exchanged documents and data with their own software, or acquire software that allows them to view exchanged documents.

This protocol attempts to simplify and reduce the cost and risk associated with the disclosure of documents by establishing standards, ensuring that the parties are in agreement as to the format of the electronic exchange.

2. Introduction

This document outlines the protocol for each party to follow for the electronic exchange of documents in the Proceeding.

Documents to be produced between the parties in the Proceeding will be exchanged electronically.

If required, parties should be able to provide court book documents electronically in the same format as previously exchanged documents. The technology to run an electronic courtroom will be negotiated at the appropriate point in time.

This Protocol set out standards, particularly for:

- Format of documents to be exchanged;
- Document Numbering;
- Fields and Data to be Exchanged;
- Data and Image Formats for Exchange;
- Updating and Re-supplying Data;
- File Integrity; and
- Responsibility for Cost.

3. Documents to be Included

This protocol encompasses the document management aspects of both hardcopy and electronic documents. This may include but is not limited to:

- Electronic Documents:

  - Emails
  - Word Documents
  - Powerpoint Presentations
  - GANTT Charts
  - Spreadsheets and financial information
  - Photographs
  - Audio / visual media
  - Internal databases
  - CAD files

- Hardcopy Documents
  - Letters
  - Contracts
  - Agreements
  - Printed emails
  - Plans
  - Facsimiles
  - Invoices
  - Minutes of meetings
  - Agendas
  - Bank statements

4. Provision of Data

The discovery will consist of:

- a load file in export.mdb format;
- documents provided as either stamped searchable PDFs or native files where the PDF is a placeholder;
- for each document, provide a text file (.txt) containing the extracted text for the corresponding native file, except where the document contains redactions, in which case a text file will be extracted from the redacted PDF of that document.

Exchange Medium

Hard drive, USB or secure file transfer

Disc Label

Name of the proceedings, the discovery tranche name and the date of provision.

5. Document Numbering

Page Numbers and Document ID

1. Every document will be assigned a unique document ID
2. Each page will have its own unique stamp. The stamp on the first page of the document will be used to identify the entire document and will be known as the Document ID.
3. The Document ID will be in the following format: AAA.BBB.FFF.PPPP_XXX. This format is described in the following table.

Level	Description
AAA	Insofar as the Respondents are concerned, the party code should consist of 3 alpha characters and represent shorthand for the party who is discovering the document. To ensure a completely unique Document ID, each party should have a different party code. Insofar as the Applicant is concerned, the party code will also consist of 3 alpha characters, the code should represent the source of the document or the relevant party's name. Refer to *"Schedule 1: Agreed Party Codes"* for a list of the agreed party codes.
BBB	The box number represents either a physical archive box or, if dealing with electronic documents, it may represent either a physical or virtual partition. The box number should comprise of 3 digits and be padded with leading zeros (0) where any number is less than 3 digits. The maximum number in any one box is 999.
FFF	The folder number is a sequential virtual folder number. Three digits should be used and should be padded with leading zeros (0) where any number is less than 3 digits. The file number should start with 001. The maximum number at this level is 999.
PPPP	It should comprise 4 digits and be padded with leading zeros (0) where any number is less than 4 digits. The maximum number at this level is 9999.
XXX	It is an optional 4 digit sequential number used after the Document ID for stamping pages of Native documents rendered to PDF. The Document ID will be stamped on the first page and the consecutive pages will be stamped with the Document ID_NNNN, with the second page starting from _0002.

6. Stamping Documents

Electronic material

Each document will be identified by applying a unique, electronically applied stamp on the top right corner every page. Where a document has been supplied in its native form, a visual stamp on that document is not required, though the document will still adopt a Document ID as a database reference.

Hardcopy material

Each document will be identified by applying a unique electronically applied stamp on the top right corner of every page. If the schema outlined in "Schedule 4: Data Format" is followed, the Document ID will not only serve as a unique identifier, but also an indicator of the physical location of the document for records management purposes.

7. Imaging

In an attempt to avoid exchanging documents in physical form, whether that be a photocopy of an original or a printed electronic document, all documents will be rendered to electronic form.

Hardcopy Material

All hardcopy documents will be scanned to fully text searchable PDF (Portable Document Format) file.

Electronically Sourced Documents

Electronically sourced documents will be converted to PDF (Portable Document Format) file.

Black and White Image Format

Images should have a resolution of between 200 to 300 DPI (dots per inch). A higher resolution may be used for images that require more detail.

Black and white images (bi-tonal) should be compressed with CCIT Group 4 compression.

Colour Image Format

Electronically sourced documents should be exchanged in colour. Hard-copy documents should be exchanged in colour only where the colour is necessary to understand the document and its relevant content.

Native Documents

Documents that are not able to be rendered to PDF should be provided in their native form. A visual stamp on the document is not required, though the native document will still adopt a document ID as a database reference.

Types of files that should be left as a native document may include, but are not limited to:

- Microsoft Access
- Microsoft Excel

- Comma Separated Text files (CSV)
- Log files
- CAD or other engineering files
- Media files (Such as mp3 or mpg)

Where an electronic document contains one or more electronic documents, each electronic document is considered a "document" in its own right and should be extracted. This may include but is not limited to .ZIP and .MSG files.

Zip files

Zip or compressed files will be uncompressed. Each file contained within a zipfile will be listed separately. The zip file container should not be processed.

Embedded files

Embedded files will be extracted from each electronic document and exchanged as separate document attachments with the following exclusions:

- The embedded file is identifiable as a graphic/ chart.
- The embedded file is identifiable as a Corporate Logo or otherwise, for example, on an email signature.
- The integrity/form of the rendered PDF should replicate that of the originating document.

Password Protected Documents

Where an electronic document is password protected, the parties will undertake reasonable efforts to provide this without such password protection or to provide the other side with the relevant

Landscape Document

Each party will endeavour to rotate all landscape documents from portrait format as so they read left to right.

Searchable Image Format

All documents will be provided as fully text searchable PDF (Portable Document Format) files. Hardcopy documents will have OCR (Optical Character Recognition) applied over the document.

Rendering of Documents to PDF Format

Should a party become aware of errors with rendering documents that party should endeavour to correct the rendering error and provide a corrected version of the document affected.

Consistency of Document Types for Electronic Documents

For hard copy paper documents refer to the Document Types in Schedule 2.

Electronic documents including email, email attachments and loose files should be given a Document Type determined by the file type as extracted by the e-processing software, e.g. "Email", "MS Word Document", "MS Excel Spreadsheet" or "MS PowerPoint Presentation".

Track Changes and Comments

If rendering native Microsoft Office documents to PDF the parties are required to show the final version of the document with track changes showing:

- Where a document is identified as containing 'Track Changes' the rendered PDF version will display the 'Track Changes' if the person reviewing the native document has 'show markup' enabled on their computer; and
- Where a document is identified as containing 'comments', the rendered PDF version will display the 'comments' if the person reviewing the native document has 'show markup' enabled on their computer

8. Redacting Documents

Privileged Documents

All documents bar those deemed as wholly privileged should be exchanged or made available for inspection. Partially privileged documents should have the privileged section(s) redacted.

Appearance of Redactions

All redactions should be made in in either black or white with a black border and the text of the nature of the redaction listed on the face of the redaction. Examples would be "Privilege – LPP" or "Privilege – WPP"

Database fields for redacted documents

To capture as much data as possible and to maximise data value, a document status of "Privileged" will be captured with an additional database field (to explain the basis for the redaction). Refer "Schedule 3: Additional Database Fields" for these fields.

9. Provision of Discovery List

Discovery list format

All documents to be exchanged between the parties in the proceedings must be provided in Microsoft Excel or searchable PDF format (or otherwise in native format). Where documents are to be provided or exchanged as searchable images, native electronic documents should be rendered directly to PDF to create searchable images. All documents to be exchanged will be described in a List of Documents containing the following information for each document:

a) Document ID;
b) Document Title;
c) Document Type;

d) Document Type;
e) Document Date;
f) Author;
g) Recipient
h) Host Reference

A list of documents is to be provided in the following format:

List	Description	Search Criteria
Schedule 1; Part 1	Not privileged This list contains all relevant documents (and document bundles) that are either not privileged , or partly privileged with partial redaction. No wholly privileged documents are included. All images and data for documents contained in this list are exchanged. Documents identified as part privileged will be provided with redactions.	Relevant = YES Privilege = NO & PART
Schedule 1; Part 2	Privileged This list contains all documents (and document bundles) that are wholly privileged. Where a relevant wholly privileged document is part of a document bundle, the document will be added to this list and will not be included in Schedule 1 – Part 1. List only is provided for these documents; no images or data are provided.	Relevant = YES Privilege = YES

10. De-duplication

Each party will take all reasonable steps to remove duplicate documents from the exchange data set (de-duplication) prior to exchange.

Terminology

When identifying duplicate documents, one document will be referred to as the Parent document and all duplicates will be referred to as Child or Children documents.

Efiles

Parties will use MD5 algorithm to identify duplicates. MD5 refers to a cryptographic hash function that outputs a unique 128-bit alphanumeric value for each file.

Emails

A separate algorithm should be used to determine duplicate emails. The hash should be created from key, standardised fields extracted from the metadata of the email, potentially including the following fields: "To", "From/Sender", "Date Sent", "Body Text", "Number of Attachments".

Document bundle handling

Where documents are in a Host/Attachment relationship (a "Bundle"), only other identical bundles are considered duplicates for removal by de-duplication.

Where an Attachment exists elsewhere, either in a different bundle or as a stand- alone file, its relationship and context is unique to itself and hence it is not a duplicate of the other document.

11. Updating and Re-supplying data

Partial updates to data set

If a party finds errors in the exchange data, the producing party will provide updated data and images for all erroneous documents. A written letter explaining why the error occurred and what documents are affected must be exchanged to all parties in the event of any re-issue of data.

Complete resupply of documents

If the erroneous data set consists of more than 25% of the entire exchanged dataset, the producing party will completely re-issue the entire data set. A written letter explaining why the error occurred and what documents are affected must be exchanged to all parties in the event of any re-issue of data.

Privilege documents exchanged

If a copy of any wholly or partly privileged documents is inadvertently disclosed by one party to another, the parties agree:

- to notify each other as soon as reasonably practicable after becoming aware of the disclosure;
- that privilege will not be waived in respect of the document by reason of the disclosure; and
- that the party receiving the document, will delete or destroy all copies of the document.

12. File Integrity

Malicious software and corrupt documents

The producing party should ensure that all documents are neither corrupted nor infected with a virus or any other malicious software.

It is the responsibility of the receiving party to check all data for malicious software prior to importing or opening the data.

Resupply of data

Documents that are corrupt or infected with malicious software will be resupplied by the producing party within 7 business days or otherwise as agreed.

13. Privilege Clawback

The parties agree that any inadvertent disclosure of privileged material shall not result in the waiver of any associated privilege nor result in a subject matter waiver of any kind.

If, when reviewing another party's disclosure material, it becomes apparent to the receiving party that some of the disclosed material may be privileged, the receiving party:

- will immediately suspend review of the apparently privileged material;
- will not make copies of the apparently privileged material; and
- will, as soon as is reasonably practicable and in any event within three business days, notify the producing party of the disclosure of the apparently privileged material.

Upon receipt of a notification made pursuant to the above, the producing party will, as soon as is reasonably practicable and in any event within three business days, either request the return of the apparently privileged material, or confirm that the disclosure of the apparently privileged material was intended.

Upon receipt of a request for the return of the apparently privileged material, the receiving party will, as soon as is reasonably practicable and in any event within three business days, return the material to the producing party with confirmation that all copies have been destroyed.

The parties agree that if the producing party does not provide any response, the disclosure of the apparently privileged material shall be deemed intended.

14. Database Format

Data will be supplied in relational Microsoft Access Database format (mdb).

Required tables

There should be the following 4 tables within each export.

Table Name	Table Description
Export:	Main document information
Parties:	People and organisation information for each document
Pages:	Listing of electronic image filenames for each document
Export Extras:	Additional data fields for each document

Refer to "Schedule 5: Tables Within Export" for a summary of the requirements for each of these 4 tables.

15. Non-compliance with Protocol

If data exchanged does not comply with this Protocol, the non-complying party may be asked to re-exchange the data in the appropriate format. This will be done at the cost of the non-complying party.

SCHEDULE 1: AGREED PARTY CODES

Party Code	Party	Legal Advisor
RIC	Richmond Valley Council, plaintiff	Quinn Emanuel Urquhart & Sullivan
JLT	Jardine Lloyd Thompson, defendant	Clayton Utz

SCHEDULE 2: DOCUMENT TYPES

Document Type
Advice
Agenda
Agreement
Affidavit
Annual Report
Announcement
Appendix
Article
Authority
Board Papers
Brochure
Certificate
Cheque
Company Search
Contract
Court Document
CV
Deed
Diagram
Diary Entry
Drawing
Email
Expert Report
Facsimile
Fax Transmission
File Note

Document Type
Financial Report
Form
Graph
Invoice
Letter
List
Manual
Map
Memorandum
Minutes
Notice
Other
Plan
Photograph
Presentation
Proposal
Questionnaire
Receipt
Report
RFI
Search
Spreadsheet
Statement
Submissions
Timesheet
Transcript
Website

SCHEDULE 3: ADDITIONAL DATABASE FIELDS in Export Extras Table

Field Name	Data Type	Character Size	Description
Privilege	PICK	255	No, Part
Privilege Basis	PICK	255	LPP or WPP
Confidential	PICK	255	Yes, No, Part
MD5	TEXT		The MD5 Hash value of the file.
Document Group	PICK	255	Host ('HWA'); Attachment ('ATT') or Unattached ('UNA').
Time	TEXT		HH:MM:SS HH is 24 hour format AEST/AEDT time zone

SCHEDULE 4: DATA FORMAT

Data and images will be provided in the following format:

1 The Folder containing all Documents will be named "\PPP\BBB\FFF\"

2 Documents produced as Searchable Images will be named "DocumentID.pdf"

3 Documents produced in Native Electronic Documents will be named "DocumentID.xxx(x)" where "xxx(x)" is the original default file extension typically assigned to source Native Electronic Files of that type. For example, Microsoft Word documents will have a ".doc" extension, Microsoft Excel files will have a ".xls" extension, so Native Files will be named along the following lines ABC.001.003.0456.xls (excel spreadsheet), XYZ.099.456.0093.doc (word document) A four character extension may be necessary for particular file types e.g. docx to cater for newer versions of Microsoft documents.

4 The Documents folder will be structured in accordance with the Document ID hierarchy for example:

4.1 The Document produced as a Searchable Image called "ABC.001.004.0392.pdf' would be located in the folder called "ABC\001\004\". So, it will appear in the directory listing as "ABC\001\004\ABC.001.004.0392.pdf'.

4.2 As per the Federal Court Guidelines dated 29 January 2009: Where this same Document has been produced as a Native Electronic Document, and, assuming for example it is a Microsoft Excel spreadsheet file, it would be called "ABC.001.004.0392.xls" and will be located in the folder called "ABC\001\004". So it will appear in the directory listing as "ABC\001\004\ABC.001.004.0392.xls".

SCHEDULE 5: TABLES WITHIN EXPORT

Table 1: Export table

Field	Data Type	Explanation – Document Type and Coding Method and possible values	
Document_ID	Text, 255	Document_ID in accordance with section 5 - ***Document Numbering***	
Document_Type	Text, 255		
		Paper Documents	Refer Document Types in Schedule 7 as determined on the basis of the face of the Document
		Electronic Documents (including email, email attachments, loose files etc)	Option 1: Document Type in Schedule 7 as determined on the basis of the face of the Document. Option 2: For electronic documents, the document type will be determined by the file type as extracted by the e-processing software, e.g. "Email", "MS Word Document", "MS Excel Spreadsheet" or "MS PowerPoint Presentation"
Document_Date	Date, 11	DD-MMM-YYYY	
		Paper Documents	Determined on the basis of the Date appearing on the face of the Document
		Undated Documents	Leave field blank

Field		Data Type	Explanation – Document Type and Coding Method and possible values	
			Incomplete Date (Month and Year only)	For example: 01-MMM-YYYY
		Emails	Electronic Metadata - Sent Date	
		Other Electronic Documents	Option1: Determined on the basis of the Date appearing on the face of the Document. Option 2: For email attachments and other electronic files, the last modified date of the file should be used where available as the date of the document (metadata extraction)	
Host_Reference	Text, 255	If the Document is an Attachment, this field contains the Document ID of its Host Document.		
Title	Text, 255	Paper Documents	Determined on the basis of the title appearing on the face of the Document	
		Email	Subject Field	
		Other Electronic Documents	Option 1 Determined on the basis of the title appearing on the face of the Document Option 2 For non-emails, the document title will be the file name of the original electronic file (metadata extraction)	
Level_1		The Party level of the Document ID (5– ***Document Numbering)***		
Level_2		The Box level of the Document ID *(5 –**Document Numbering)***		
Level_3		The Folder level of the Document ID (5 - Document Numbering) under which the Searchable Images or Native Electronic Documents are stored		

Table 2: Pages table

Field Name	Data Type	Field Type	Description
Document_ID	TEXT	255	Document ID
Image_File_Name	TEXT	128	The File Name including the extension.
Page_Label	TEXT	32	Page number. If document is supplied in native format, then the field should be populated with "NATIVE"
Page_Num	NUMBER	DOUBLE	The sequencing numbers ensuring the pages are in the correct order. For example, the first page of the document will be 1, the second will be 2, the third 3 etc.

Table 3: Parties table

Field	Data Type	Explanation - Document Types and Coding Method and possible values	
Document_ID	Text, 255	Document ID in accordance with paragraph 31	
Correspondence Type	Text, 100	Correspondence Type (Sent or Received)	
		Paper Documents	AUTHOR, RECIPIENT BETWEEN, ATTENDEES, CC To be determined on the basis of the face of the Document
		emails	FROM, TO, CC, BCC To be determined on the basis of the face of the Document
		Other Electronic Documents	AUTHOR, RECIPIENT, BETWEEN, ATTENDEES. CC Option 1 To be determined on the basis of the face of the Document. Option 2 The parties' information will be in the format as extracted from the document metadata
Organisations	Text, 255		

Field	Data Type	Explanation - Document Types and Coding Method and possible values	
		Paper Documents	Name of organisation that produced the Document as determined on the basis of the face of the Document
		emails	Determine the field on the basis of the face of the Document
		Other Electronic Documents	Option 1 To be determined on the basis of the face of the Document Option 2 This information will be in the format as extracted from the document metadata
Persons	Text, 255		
		Paper Documents	To be determined on the basis of the face of the Document
		emails	Electronic Metadata - email addresses or email alias names
		Other Electronic Documents	Option 1: Determined on the basis of the face of the Document Option 2: This information will be in the format as extracted from the document metadata

Table 4: Export extras table

Field Name	Data Type	Character Size	Description
Document_ID	TEXT	255	Document ID
The Category	TEXT	50	• TEXT, or • DATE, or • NUMB, or • BOOL, or • PICK
The Label	TEXT	255	The name of field
The Value	TEXT	255	Content of the Field for TEXT, NUMB, DATE and PICK values only. DATE to appear in format "DD-MMM-YYYY"
Text Value	TEXT	255	TEXT or PICK field data only
Memo Value	MEMO	NA	MEMO field data only
Date Value	DATE	NA	DATE field data only in format "DD-MMM-YYYY"
Bool Value	NUMBER	LONG INTEGER	Content of the field for BOOL data. "O" is false, -1 or 1 is true
Numb Value	NUMBER	DOUBLE	NUMB field data only