* ***This Protocol is designed to be used in the jurisdiction of England and Wales, though it can be employed in any situation where all involved parties agree to its use.***
* ***This Protocol should be used to record the result of discussions between the parties on the mechanics of disclosure. If the matter falls within the remit of the Disclosure Pilot for the Business and Property Courts in England and Wales, that came into force on 1st January 2019, it is recommended that this this Protocol should so far as possible be finalised with the completed Disclosure review Document, that is to say 5 days before the first CMC. If this is not possible it should finalised no less than 7 days prior to the date of exchange.***
* ***This Protocol is not a contractually binding legal agreement between the parties. It is recognised that circumstances may arise which may make it appropriate for there to be variations to the matters set out in this Protocol. Such variations should be agreed with the other party or parties.***
* ***This protocol should be completed with reference to its parallel document; “Guidelines to eDisclosure Exchange Protocol”.***
* ***Please email any feedback to ILTAprotocol@iltanet.org***

1. **MATTER DETAILS**

|  |  |
| --- | --- |
| Party drafting protocol |  |
| Party or Parties agreeing protocol |  |
| Matter Identification |  |
| Exchange Date (if known) |  |
| [Any other significant date/milestones] |  |

1. **PROTOCOL COMPONENTS**
   1. Each party's electronic disclosure should consist of the following:
   2. A Disclosure List containing, in tabular form, details of all disclosed documents (see section 3 below).
   3. Electronic copies of the listed documents for inspection/loading by the other side (see section 4 below).
   4. A "data exchange file" (or "load file") containing metadata and other information relating to the disclosed documents (see sections 5 to 7 below).
2. **DISCLOSURE LIST**
   1. The “Disclosure list” will be provided as an [Excel spreadsheet / Word table]. It will contain all of the documents to be disclosed, sorted in a chronological fashion which ensures that any attachments (where the parent is also present) will be listed directly below their parent. All documents will be assigned a unique Disclosure Number. The list will contain, as a minimum, the fields set out below. Additional fields, may be supplied depending upon their availability and agreement with the other party for similar disclosure either in the Disclosure List or the load file.
   2. The following terms apply to the protocol
   * **Email** : Email and attachments.
   * **ESI** : Electronically Stored Information. Sometime known as eDocs or electronic documents. Includes Microsoft Office formats such as Word, Excel, PowerPoint, etc. Could also include other forms of data such as text messages, WhatsApp, Messenger, Yammer, etc.
   * **Native** : In the case of email data, the term native will refer to a format in which all of the associated metadata, email header information, [attachments] and email structure is preserved within the electronic file. For other ESI the term native will refer to the original format of the data.
   * **Metadata** : The term metadata will refer to the “data about data” information that is held within native files. It is information for example about how, when and by whom it was received, created, accessed, modified and formatted. Metadata is not normally removed or redacted, if this is the case, it should be notified to the receiving party. Metadata is supplied on an “as is” basis.
   * **Image** : The term image will refer to the format in which non-native files will be produced. Images are mainly used where an item requires redaction, though they might also be provided as the result of scanning hard copy documents.
   * **Text** : The term text will refer to the text provided alongside images. The text will reflect the information contained within the body of the image, except for redacted elements which will not be shown within the text file.

|  |  |
| --- | --- |
| **Field** | **Description** |
| [Insert field name here] | This will be a unique number to both identify all documents and to allow for documents to be matched up with their metadata in the DAT load file. For documents supplied in an image format, the this number will be used in the image *.opt* file.  **Format :** XXX000001 (3 letters, followed by 6 digits, using leading zeros.)  **Note :** Parties should agree on the text prefix (XXX) before exchanging, each party should use a different text prefix to ensure there is no duplication of Beg Bates. **We propose to use [ ].** |
| [Insert field name here] | As for previous field, except identifies the end of the document. |
| [Insert field name here] | As for the first row, except identifies the family relationship between documents. For all attachment documents, the value of this field is inherited from the start of the parent document. |
| [Insert field name here] | As for second row, except identifies the end of the family group. For all attachment documents, the value of this field is inherited from the end of the parent document. |
| [Insert field name here] (Date & Time) | For all emails date and time are in a single field in the following format   * DD/MM/YYYY HH:MM e.g. 19/02/2005 15:37 * 24 Hour clock GMT * If no date is available the field value will be blank   Note that for attachments to emails this field will be set to the date/time of the parent. |
| **OR** | |
| [Insert field name here] (Date only) | Date in a single field in the following format   * DD/MM/YYYY e.g. 19/02/2005 * If no data is available the field value will be blank   Note that for attachments to emails this field will be set to the date of the parent. |
| [Insert field name here] (Time only) | Time in a single field in the following format   * HH:MM e.g. 15:37 * 24 Hour clock GMT * If no data is available the field value will be blank   Note that for attachments to emails this field will be set to the time of the parent. |
| [Insert field name here] (Date & Time) | For all documents, date and time in a single field in the following format   * DD/MM/YYYY HH:MM e.g. 19/02/2005 15:37 * 24 Hour clock GMT * If no date is available the field value will be blank |
| **OR** | |
| [Insert field name here] (Date only) | Date in a single field in the following format   * DD/MM/YYYY e.g. 19/02/2005 * If no data is available the field value will be blank. |
| [Insert field name here] (Time only) | Time in a single field in the following format   * HH:MM e.g. 15:37 * 24 Hour clock GMT * If no data is available the field value will be blank |
|  |  |
| [Insert field name here] | Description of the electronic file type .e.g. .MS Word. |
| [Insert field name here] | Description of the electronic file extension .e.g. .doc or .docx. |
| [Insert field name here] | Email : **Subject** - extracted from meta data |
| [Insert field name here] | ESI : File name, i.e. “Important Document.doc” |
| [Insert field name here] | Email : **From** - extracted from meta data. |
| [Insert field name here] | Email : **To** - extracted from meta data. |
| [Insert field name here] | Email : **CC** - extracted from meta data. |
| [Insert field name here] | Email : **BCC** - extracted from meta data. |
|  |  |
| Additional fields as agreed | |
| [Issues] | Issue codes |
| [Relevance] | Relevant / Not Relevant |
| [Redacted] | Yes / No / blank |
| [Placeholder] | Yes / No / blank |

1. **ESI FORMATS / PROTOCOL CONVENTIONS**
   1. The production [will / will not] be employing placeholders. If placeholders are being used, they will be a single page [tiff image / PDF] with appropriate wording to reflect the following circumstances:

* [Where an entire document is being withheld for reasons of privilege, a placeholder will be inserted instead of completely redacted pages.]
* [To indicate the presence of non-relevant children within email families.]
* [To indicate the presence of a non-relevant parent within email families.]
* [To indicate the presence of a native file that is being produced as an image in order to prevent the disclosure of specific meta-data.]
  1. Where available, all documents should be disclosed in their native format, unless there has been a need to image in order to apply redactions . Where this is the case, the documents will be received/ provided as [redacted single/multi page [TIFF images / PDF’s]].
  2. In email groups were there are irrelevant children or parents, the group [will not be produced in its entirety. / will be produced in its entirety in order to provide context [In such cases the Relevance field will be used to show if a document is relevant or not]].
  3. In email groups relevant parents with irrelevant and/or redacted children [will be produced in native format / [will not be produced in native format. This might result in the splitting of family associations, if this the case the information in the Date field, can be used to re-group family items]].
  4. In email groups, the irrelevant parent of relevant children [will be produced. / will not be produced]. If disclosed they will be produced as an [image / placeholder].
  5. Relevant and fully privileged documents [will not be produced / will be represented by a placeholder if part of an email group]. If all an email group is considered Privileged, it will not be disclosed nor represented by placeholders.
  6. Imaged documents will be provided with an associated text file containing either the extracted text or OCR resulting from a scanning process. These should be in the form of one text file per documents and should be referenced in the load file via a relative path. This information will be included in the disclosure on an “as-is” basis, in accordance with paragraph 34 of CPR Practice Direction 31 B.
  7. If paper documents have been scanned, they will be supplied as text searchable [TIFF images / PDF’s]. Documents [will / will not] be supplied with objective coding.

1. **LOAD FILE FORMAT**
   1. The load file will be in DAT format using the protocols and delimiters shown below
   2. The following protocols will be followed.

* All native ESI will be referenced in the DAT file by way of a relative link to the ESI.
* All extracted/OCR text files referenced in the DAT file by way of a relative link to the file.
* The DAT file will be provided in UTF-8 format.
* Images will be provided by way of an Opticon .opt load file.
  1. We propose to use the following industry-standard delimiters for the DAT file

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Details** | **Character** | **ASCII Code** | **Unicode (hex)** |
| Text Qualifier | Contains the contents of an entire field | þ | 254 | 00FE |
| Field Delimiter | Separates individual fields on the list |  | 020 | 0014 |
| Multi-value Delimiter | Separates multiple values on one field | ; | 059 | 003B |

1. **LOAD FILE CONTENTS**
   1. The load file will consist of the information detailed in the Disclosure list and the following data.

|  |  |
| --- | --- |
| **Field** | **Description** |
| MD5 Hash  (EF\_MD5HASH) | To be generated for all emails and ESI. Enables parties to identify exact duplicates possessed and exchanged by all. |
| Native Path  (ProductionNativePath) | Path of delivered native files for electronic documents (standalone non-redacted documents) or for PDF’s for paper documents, e.g.  .\VOL001\NATIVES\NATIVE00001\XXX\_000000333.pdf |
| Extracted/OCR Text  (ProductionTextPath) | Path of delivered text files, e.g.  .\VOL001\TEXT\TEXT00001\XXX\_000000333.txt |
|  |  |
| *Image Path*  *(ProductionImagePath)* | *Path of delivered image files, e.g.*  *.\VOL001\IMAGES\IMAGES00001\XXX\_000000333.tif* |
| Additional fields as agreed |  |

1. **EXCHANGING DATA**
   1. Each party is to provide their data via a suitably secure mechanism. [If requested, we can provide access to our secure FTP site for the receipt of opposing parties disclosure.]
   2. Our data exchange will normally be conducted via our secure FTP site. Where this is not used, information will be physically exchanged via encrypted media (memory stick or hard drive).
   3. The medium used should be encrypted using a recognised data encryption tool with a minimum of 256 bit encryption and using a complex password, which will be sent via a separate email.