MUSEUM DATA SERVICE

Museum Data Service
Data Processing Agreement

PARTIES:

(1) **The Public Catalogue Foundation**, a charitable company incorporated in England and Wales with company number 04573564, whose registered address is Salisbury House, Station Road, Cambridge, England, CB1 2LA, and whose trading name is Art UK (the 'Data Processor'); and

(2)

Organisation name	(the 'Data Controller')
Type of company and jurisdiction of registration	
Company number (if any)	
Registered address	
Trading name (if any)	

(each a 'Party' and together the 'Parties').

WHEREAS:

(A) The Data Controller intends to provide certain collection data and certain metadata (the 'Data Collection') to the Data Processor under the terms of a separate data collection deposit agreement to be entered into by the Parties (if applicable) for the benefit of the joint venture between the Data Processor, Collections Trust and the University of Leicester known as the Museum Data Service (or such name as the Charity Commission may agree) ('MDS').

(B) This Agreement shall govern any processing of any Personal Data contained in the Data Collection and is intended to ensure that any Personal Data contained within the Data Collection is processed in accordance with applicable Data Protection Law.

(C) The Parties acknowledge that as at the date of this Agreement, MDS has not yet been established and the Parties acknowledge and agree that the rights, obligations and liabilities of the Data Processor under this Agreement shall be transferred to MDS once it has been established.

IT IS AGREED:

1. Definitions and interpretation

1.1 In this Agreement:

'Data Protection Law': means the Data Protection Act 2018 and "the UK GDPR" which is defined in section 3(10) of the Data Protection Act 2018 and supplemented by section 205(4).

The terms 'Controller', 'Personal Data' and 'Processor' shall have the meaning ascribed to such terms in the Data Protection Law. Where this Agreement use the terms defined in the UK GDPR and/or the Data Protection Act 2018 respectively, those terms shall have the same meaning as in that legislation.

1.1 In this Agreement, unless the context requires otherwise:

(a) references to a person include any individual, firm, body corporate (wherever incorporated), government, state or agency of a state or any joint venture, association, partnership, works council or employee representative body (in any case, whether or not it has separate legal personality);

(b) references to a paragraph, Section or Schedule are to those of this Agreement;

(c) headings do not affect its interpretation;

(d) the singular shall include the plural and vice versa, and references to one gender include all genders;

(e) references to any English law legal term or concept shall, in respect of any jurisdiction other than England and Wales, be construed as references to the term or concept that most nearly corresponds to it in that jurisdiction;

(f) any phrase introduced by the terms including, include, in particular or any similar expression shall be construed as merely illustrative and shall not limit the sense of the words preceding those terms; and

(g) references to 'applicable law', 'law' or 'laws' shall mean (i) any statute, regulation, by-law, or subordinate legislation; (ii) the common law and the law of equity; (iii) any binding court order, judgment or decree; or (iv) any industry code, policy or standard enforceable by law.

2. Inconsistencies

If there is any inconsistency between any definition set out in a Schedule and a definition set out in any clause or any other Schedule, then, for the purposes of construing that clause or Schedule, the definition set out in that clause or Schedule shall prevail.

3. Processing of Personal Data

3.1 The Data Controller instructs the Data Processor to process Personal Data as necessary to provide the Museum Data Service ('Service') (including to improve and update the Service, for security or business continuity purposes, troubleshooting and support, accounting purposes, and to carry out processing initiated by the Data Controller users) and to perform the Data Processor's obligations and exercise its rights under this Agreement.

3.2 The details of the processing operations, in particular the categories of Personal Data and the purposes of processing for which the Personal Data is processed on behalf of the Data Controller, are specified in Schedule 1.

3.3 Each Party will comply with the obligations applicable to it under the Data Protection Law with respect to the processing of Personal Data.

3.4 Data Controller is responsible for ensuring compliance with the relevant laws and establishing the legal basis for processing, some of the applicable legal basis for this processing are set out in Schedule 1.

4. Instructions

4.1 The Data Processor shall only process Personal Data: (a) on the Data Controller's written instruction; and (b) as required by applicable law.

4.2 If the Data Processor is required to process the Personal Data under applicable law, it shall inform the Data Controller of that legal requirement before processing the Personal Data, unless the law prohibits this on important grounds of public interest.

4.3 The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, instructions given by the Data Controller infringe Data Protection Law.

5. Purpose limitation

The Data Processor shall process the Personal Data only for the specific purpose(s) of the processing, as set out in Schedule 1, unless it receives further written instructions from the Data Controller.

6. Duration of the processing of Personal Data

Processing by the Data Processor shall only take place for the duration specified in Schedule 1.

7. Security of processing

7.1 The Data Processor will implement and maintain technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Schedule 1 (Security), taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Data Processor may update or modify the technical and organisational measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service.

7.2 The Data Processor shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the Service. The Data Processor shall ensure that persons authorised to process the Personal Data received have committed themselves to appropriate confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

7.3 Where the Data Controller grants access to the Personal Data held in the Service, the Data Controller must ensure that those persons it has authorised will adhere to any security controls or procedures.

8. Use of sub-Processors

8.1 The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors from an agreed list (Schedule 2). The Data

Processor shall specifically inform in writing the Data Controller of any intended changes of that list (Schedule 2) through the addition or replacement of sub-processors at least one month in advance, thereby giving the Data Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Data Processor shall provide the Data Controller with the information necessary to enable the Data Controller to exercise the right to object.

8.2 Where the Data Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Data Controller), it shall do so by way of a written contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Data Processor in accordance with this Agreement. The Data Processor shall ensure that the sub-processor complies with the obligations to which the Data Processor is subject pursuant to this Agreement and to the Data Protection Law.

8.3 At the Data Controller's request, the Data Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Data Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Data Processor may redact the text of the agreement prior to sharing the copy.

8.4 The Data Processor shall remain fully responsible to the Data Controller for the performance of the sub-processor's obligations in accordance with its contract with the Data Processor. The Data Processor shall promptly notify the Data Controller of any failure by the sub-processor to fulfil its contractual obligations.

8.5 In the event the Data Processor has factually disappeared, ceased to exist in law or has become insolvent the Data Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

9. International transfers

Any transfer of Personal Data outside of the UK by the Data Processor shall be done only on the following conditions: (a) in accordance with Section 3.14.1; and (b) the transfer will be: (i) to a country with an "adequacy finding" by the UK; (ii) the transfer will be covered by an appropriate safeguard, such as the UK's International Data Transfer Agreement (ITDA) or the UK's International Data Transfer Addendum to the EU's new Standard Contractual Clauses (SCC); or (iii) the transfer will be covered by a derogation in the UK GDPR or an exemption in the Data Protection Act 2018.

10. Documentation and compliance

10.1 The Parties shall be able to demonstrate compliance with this Agreement.

10.2 The Data Processor shall deal promptly and adequately with inquiries from the Data Controller about the processing of Personal Data in accordance with this Agreement.

10.3 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations that are set out in this Agreement and stem directly from the Data Protection Law. At the Data Controller's written request, the Data Processor shall also permit and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Data Controller may take into account relevant certifications held by the Data Processor.

10.4 The Data Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Data Processor and shall, where appropriate, be carried out with reasonable notice.

10.5 The Parties shall make the information referred to in this Agreement, including the results of any audits, available to the competent supervisory authority/ies (in the UK this is the Information Commissioner's Office) on written request.

10.6 The Data Processor must also give the Data Controller whatever information it needs to ensure both Parties are meeting their Article 28 and Article 32 obligations under the UK GDPR.

11. Assistance to the Data Controller

11.1 The Data Processor shall promptly notify the Data Controller of any request it has received from a data subject to exercise any of their rights under the Data Protection Law. The Data Processor must not respond to the request itself, unless authorised to do so by the Data Controller.

11.2 The Data Processor shall assist the Data Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights under Data Protection Law, taking into account the nature of the processing. In fulfilling its obligations in accordance with this Section 11 the Data Processor shall comply with the Data Controller instructions.

11.3 The Data Processor shall assist the Data Controller in responding to, or cooperating with, the UK Information Commissioner's Office in relation to any matter concerned with this Agreement.

11.4 In addition to the Data Processor's obligation to assist the Data Controller pursuant to this Section 11, the Data Processor shall assist the Data Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Data Processor:

(a) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(b) the obligation to consult the competent supervisory authority/ies (in the UK this is the Information Commissioners Office) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk; and

(c) the obligation to ensure that personal data is accurate and up to date, by informing the Data Controller without delay if the Data Processor becomes aware that the Personal Data it is processing is inaccurate or has become outdated.

(d) any other obligations as specified in Data Protection Law.

12. Notification of Personal Data breach

In the event of a Personal Data breach, the Data Processor shall promptly cooperate with and assist the Data Controller for the Data Controller to comply with its obligations under Data Protection Law, where applicable, taking into account the nature of processing and the information available to the Data Processor.

13. Data breach concerning data processed by the Data Controller

13.1 In the event of a Personal Data breach concerning data processed by the Data Controller, the Data Processor shall, to the extent it is able to do so, assist the Data Controller:

(a) in notifying the Personal Data breach to the competent supervisory authority/ies, without undue delay after the Data Controller has become aware of it, where relevant (unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons),

(b) in obtaining the following information which, pursuant to Data Protection Law, shall be stated in the Data Controller's notification, and must at least include:

(i) the nature of the Personal Data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(ii) the likely consequences of the Personal Data breach;

(iii) the measures taken or proposed to be taken by the controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(c) in communicating without undue delay the Personal Data breach to the data subject, when the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons.

13.2 Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

14. Data breach concerning data processed by the Data Processor

14.1 In the event of a Personal Data breach concerning data processed by the Data Processor, the Data Processor shall, without undue delay, provide the Data Controller with the following information:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the Personal Data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the Personal Data breach, including to mitigate its possible adverse effects.

14.2 Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

14.3 Following any Personal Data breach, the Parties will co-ordinate with each other to investigate the matter.

15. Non-compliance with this Agreement

Without prejudice to any provisions of Data Protection Law, in the event that the Data Processor is in breach of its obligations under this Agreement, the Data Controller may instruct the Data Processor to suspend the processing of Personal Data until the Data Processor complies with this Agreement or may terminate this Agreement in accordance with Section 18.3. The Data Processor shall promptly inform the Data Controller in case it is unable to comply with this Agreement, for whatever reason.

16. Successors and assigns

16.1 This Agreement is binding on and will benefit the successors and assigns of the Parties.

16.2 Subject to Section 16.3, either Party may assign or transfer any of its rights and obligations under this Agreement and shall give promptly notice of the same in writing to the other Party.

16.3 If a Party assigns or transfer any of its rights or obligations under this Agreement then:

(a) the other Party shall have no greater liability under this Agreement than it would otherwise have had; and

(b) the other Party shall, on request from that Party, execute any agreement or other instrument (including any supplement or amendment to this Agreement) that may be required to give effect to or perfect the assignment or transfer.

17. Term

This Agreement shall come into effect on the date of this Agreement and shall continue thereafter for so long as the Data Processor is processing any Personal Data in the Data Collection unless and until either Party terminates this Agreement under Section 18.

18. Termination and consequences of termination

18.1 If within three months of signing this Agreement the Parties do not also enter into a Data Deposit Agreement, this Agreement shall automatically terminate.

18.2 If the Data Deposit Agreement expires or terminates for whatever reason, this Agreement shall automatically terminate.

18.3 The Data Controller may terminate this Agreement for Agreement any breach of the terms of this Agreement or Data Protection Legislation by the Data Processor or by anyone employed by it or acting on its behalf immediately (without prior written notice).

18.4 Either Party may terminate this Agreement by giving not less than six calendar months' notice in writing to the other Party. Where the Party providing such notice is the Data Processor, the Data Processor shall provide notice of termination of any agreement relating to sub-processing to any Data Sub-processor and shall procure that no sub-processing takes place following termination of this Agreement.

18.5 Following termination of the Agreement, the Data Processor shall within 30 days either, at the choice of the Data Controller, delete any Personal Data processed on behalf of the Data Controller and certify to the Data Controller that it has done so, or

return any such Personal Data to the Data Controller and delete existing copies unless applicable laws require further storage of the Personal Data.

18.6 Until the data is deleted or returned, the Data Processor shall continue to ensure compliance with this Agreement.

19. Limitations of liability

19.1 Notwithstanding any other provision of this Agreement, neither Party shall be in breach of, or under any liability to the other Party in respect of, this Agreement to the extent that the breach or liability arises as a result of any breach by the other Party of its obligations under this Agreement.

19.2 The Data Processor shall not be liable to the Data Controller for:

(a) any loss of profits, revenue, contracts, business, anticipated savings, goodwill or reputation, in each case whether direct or indirect; or

(b) any costs that are not reasonably foreseeable or any loss or damage of any kind that is, in either case, indirect or consequential,

in each case, whether in contract (including under any indemnity or warranty), tort, or otherwise, that arise under or in connection with this Agreement.

19.3 The aggregate amount of the liability of the Data Processor under this Agreement for any costs, expenses, loss or damage arising from or relating to any claim under, or breach of, this Agreement shall not exceed £2,500.

19.4 The limitations in Sections 19.2 and 19.3, shall not apply to a Party's liability:

(a) for fraud or fraudulent misrepresentation;

(b) for death or personal injury caused by its negligence; or

(c) any other liability that cannot be excluded by applicable law (including Data Protection Law).

20. Notices

20.1 Any communications or notices relating to this Agreement shall be given via email, using the email addresses given under the signature of:

(a) in the case of communications or notices to the Data Controller, the Data Controller's representatives on the signature page of this Agreement instead of by post to the Data Controller's registered address; and

(b) in the case of communications to the Data Processor, the Data Processor's representatives on the signature page of this Agreement, or via support@museumdata.uk, instead of by post to the Data Processor registered address.

20.2 A communication shall be effective upon receipt and shall be deemed to have been received at the time of transmission of the email. Where delivery occurs outside Working Hours, notice shall be deemed to have been received at the start of Working Hours on the next following Business Day.

20.3 Each Party shall notify the other Party in writing of a change to its details referred to in this Section 19 from time to time.

21. Whole agreement

This Agreement sets out the whole agreement between the Parties in respect of the subject matter of this Agreement and supersedes any previous draft, agreement, arrangement or understanding, whether in writing or not, relating to its subject matter.

22. Variation

22.1 Except as otherwise set out in this Agreement, no variation will be effective unless in writing signed by or on behalf of both Parties.

22.2 If this Agreement is varied:

(a) the variation shall not constitute a general waiver of any provisions of this Agreement;

(b) the variation shall not affect any rights, obligations or liabilities under this Agreement that have already accrued up to the date of variation; and

(c) the rights and obligations of the Parties under this Agreement shall remain in force, except as, and only to the extent that, they are varied.

23. Severability

23.1 Each of the provisions of this Agreement is severable.

23.2 If, and to the extent that, any provision of this Agreement:

(a) is held to be, or becomes, invalid or unenforceable under the applicable law or any jurisdiction; but

(b) would be valid, binding and enforceable if some part of the provision were deleted or amended,

then the provision shall apply with the minimum modifications necessary to make it valid, binding and enforceable and neither the validity or enforceability of the remaining provisions of this Agreement, nor the validity or enforceability of that provision under the law of any other jurisdiction, shall be in any way affected or impaired.

24. Legal relationship

This Agreement does not create any partnership or joint venture between the Parties nor make either Party the agent of the other Party for any purpose.

25. Waiver

25.1 No delay, neglect or forbearance by either Party in enforcing its rights under this Agreement or provided by law shall be a waiver of or prejudice of those rights. The single or partial exercise of any right under this Agreement or provided by Law shall not preclude any further exercise of it.

25.2 No waiver of any breach of any provision of this Agreement shall constitute a waiver of any other breach of the same or any other provision, and no waiver shall be

effective unless made in writing and signed by an authorised representative of the waiving Party.

26. Counterparts

This Agreement may be executed in any number of counterparts, and by each Party on separate counterparts. Each counterpart is an original, but all counterparts shall together constitute one and the same instrument.

27. Governing law and jurisdiction

This Agreement and any non-contractual obligations arising out of, or in connection with, it shall be governed by, and interpreted in accordance with, the laws of England and Wales. Each Party irrevocably submits to the exclusive jurisdiction of the English courts in relation to any dispute that may arise concerning this Agreement, which shall be decided by the High Court.

IN WITNESS of which this Agreement has been executed by or on behalf of each Party.

SIGNATURES

Authorised to sign for and on behalf of

THE PUBLIC CATALOGUE FOUNDATION

Signature	
Print name	
Occupation	
Email	
Date	

Authorised to sign for and on behalf of

Signature	
Print name	
Occupation	
Email	
Date	

Schedule 1 – Details of processing

This Schedule includes certain details of the processing of Personal Data covered by this Agreement as required by Article 28(3) of the UK GDPR.

Nature of the processing	Provision of the Museum Data Service
Categories of Data Subjects whose Personal Data is processed	Employees and volunteers of the Data Controller, and other specific individuals given user access permissions to the Data Controller's Museum Data Service account. Individuals whose Personal Data is included within records exported by the Data Controller from its collections data and deposited with the Museum Data Service.
Categories of Personal Data processed	Most Personal Data processed will not include any in the special categories defined by UK GDPR. However, in some cases individual object records may contain special category data relevant to the history or significance of items in museum collections. Examples might include the ethnic origins, political opinions, religious beliefs, trades union membership or sexual orientation of individuals who made, owned or are otherwise associated with specific objects. In these cases, the Data Controller is responsible for ensuring necessary steps have been taken to comply with Data Protection Law.
Lawful Basis for processing	Museums will largely rely on the following legal bases for processing collections data, depending on the nature of their organisation: If they are a public authority as set out in Schedule 1 of the Freedom of Information Act 2000, their legal basis for processing collections data will be GDPR Article 6 (1) (e), where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (commonly known as the 'public task' exemption). A museum that is not a public authority may in some circumstances rely on the 'public task' exemption, but in most cases will rely on GDPR Article 6 (1) (f), necessary for the purposes of the legitimate interests pursued by the controller, balanced against the rights and freedoms of the data subject. Museums may choose to rely on other legal basis at their discretion.

Purpose(s) for which the Personal Data is processed on behalf of the Data Controller	Until a Data Deposit Agreement is signed between the Parties, any Personal Data contained within records deposited with the Museum Data Service is processed only to help the Data Processor analyse the whole deposited dataset. This will result in an annex to the Data Deposit Agreement in which the Data Controller will specify one of four levels of access permission for each field containing Personal Data. Depending on the access permissions specified by the Data Controller in the Data Deposit Agreement, the purpose(s) for which any Personal Data is processed may include: • maintaining a back-up copy of collections data to help with disaster recovery; • providing remote access to selected third parties (including employees and volunteers of the Data Controller, and other specific individuals given user access permissions to the Data Controller's Museum Data Service account) for research, interpretation and other collections-based activities. Such third parties will only be provided access by the Data Processor at the written instruction of the Data Controller. Alternatively, access may be provided to third parties by being granted directly by the Data Controller.
Duration of the processing	Personal Data will continue to be processed until this Agreement is terminated, plus 30 days to enable the Data Processor to delete the Personal Data (unless Data Protection Law requires further storage of the Personal Data).
Security measures	The technical core of the Museum Data Service is the CIIM middleware developed by Knowledge Integration Ltd ('the MDS CIIM'). Access to the MDS CIIM is limited to authorised, logged-in users, using Keycloak to authenticate log-ins. Upon the signing of this Agreement, the Data Processor will create a secure account for the Data Controller within the MDS CIIM. The profile settings for this account will include a named representative of the Data Controller authorised to administer the account. At first, the Data Controller's data (including Personal Data) will only be accessible to logged-in users authorised by the Data Processor and to the Data Controller's nominated representative.

	If depositing data via a file exported from a collections database, the nominated representative will upload this file directly to the Museum Data Service via the Data Controller's secure account. No export file containing Personal Data may be emailed or transferred via any third-party file-sharing platform. In the Data Deposit Agreement, the Data Controller will specify the access permission levels for any field in the deposited data that cannot be made available to anyone, whether logged into the MDS CIIM or not. The Data Deposit Agreement will specify one of three access permission levels for each non-public field: • Administrator • Restricted confidential • Restricted non-confidential The Data Processor will apply the specified access permissions, and these will be reflected in the indexes. For example, no data from non-public fields will be included in the index used for public searching. The Data Controller's nominated representative will use their MDS CIIM dashboard to manage the list of users authorised to access non-public fields.

Schedule 2 – Sub-processors

1. Knowledge Integration Ltd, company registration number 03878083, whose registered address is Paradise House, 35 Paradise Street, Sheffield, S3 8PZ.
2. Collections Trust, company number 01300565, whose registered address is Rutland House, 23-25 Friar Lane, Leicester LE1 5QQ.
3. University of Leicester, whose principal place of business is on University Road, Leicester LE1 7RH.