QUOTE

DATE: 09/11/23
VAT NUMBER: 363997344

41 Sheep Walk
Shepperton
Surrey
TW17 0AU

[redacted]

Customer Address

[redacted]
The Cabot
25 Cabot Square
London
E14 4QZ

REFERENCE	ACCOUNT NUMBER	PERIOD
OFJ12425	CMA	20 November 2023 - 20 November 2023 Delivery: 20 November 2023

[redacted]

[redacted]

NET TOTAL	£14,569.00
VAT (20%)	£2,913.80
TOTAL	£17,482.80

CONDITIONS OF SALE

1. All Services and advice are provided without warranty or guarantee of any kind and as such we cannot be held responsible for any financial losses or any additional costs associated however incurred
2. This sale may be subject to additional transport costs as a result of fulfilling this sales. Where possible the customer will be notified of these costs however the customer agrees to pay reasonable transport costs without discussion.
3. The customer is required to pay the full invoice charges within the terms of the invoice. Where not specified these terms are 28 days.
4. If the payment is deemed late then the customer will be charged interest on the outstanding balance at a rate 8% above the Bank of England base rate. In addition the customer is liable for administration cost not exceeding £100 and any legal expenses resulting from recovery of the dept.
5. All quotes provided by OFilms are valid for 60 days from date on quote.
6. The amount quoted by OFilms is restricted for equipment and services listed by the quote. Any changes may be subject to additional costs.

CONDITIONS OF HIRE

1. All equipment hired remains the property of OFilms.
2. Hire charges apply for the period of the contract regardless of whether the equipment is in use.
3. The hire period commences upon delivery and ends once the equipment has been returned and inspected by OFilms.
4. Equipment hired will be entirely at the customers risk during the hire period. The customer is fully responsible for any loss or damage. The customer undertakes responsibility for insuring equipment against “all risks” to the full replacement value. Any loss or damage to the equipment is to be reimbursed to OFilms by the customer to the full replacement value. In addition the customer undertakes to pay the full hire charge for the duration of the period until the equipment is returned to OFilms in full working order.
5. The customer is required to pay the full invoice charges within the terms of the invoice.
6. In the event that the equipment is returned late and not at the end of the agreed hire period OFilms will charge an additional hire period at the full hire rate excluding discounts.
7. The customer undertakes to adhere to relevant regulations, rules or statutory provisions governing, or relating to, the use of any hired equipment.
8. Equipment will be supplied to the customer in fully working order. OFilms will only accept liability for defect or failure arising from normal use.
9. The customer undertakes to use the equipment in a manner which will not cause undue damage or deterioration to the equipment. The customer is responsible for rectifying damage caused by improper use.
10. It is the responsibility of the customer to take all measures to avoid personnel injury or damage resulting from improper use of any hired equipment.
11. The hired equipment must not be altered or modified by the customer in any way.
12. Any damage to or failure of the equipment must be reported to OFilms within 24 hours.
13. OFilms must be made aware of the location of any hired equipment at all times.
14. The customer must not hire to a third party any equipment which is the property of OFilms.
15. The customer should make every effort to return the hired equipment in the condition it was received. OFilms reserves the right to charge for any additional work required to return the equipment to this condition. If it is not possible to return the equipment to the received condition then a replacement cost will be charged. The following is examples of work which might incur additional costs to the customer.
    1. Cut cables
    2. Re-wired connectors, plugs, sockets
    3. Old tape left on equipment
    4. Incorrectly coiled cables
    5. Damaged connectors
    6. Dents in housings
    7. Exceptional dirt, mud or other substances
    8. Cleaning and removal of Haze fluid
16. OFilms has the right to terminate the hire and/or reposes its property if any of the terms of this agreement and the accompanying documents are not met.

STREAMING & DOWNLOADS

1. Ofilms will only be responsible for the equipment they are providing (unless agreed in writing). Ofilms is not responsible for 3rd Party software, 3rd Party CDNs (YouTube, Vimeo etc.), 3rd Party internet connections and 3rd Party video equipment unless we are providing it.
2. The customer will make sure that all material provided for streaming or download wil have the relevant copyright or be copyright free
3. This sale may be subject to additional data and usage charges.

NETWORKS

1. Ofilms is only responsible for the part of the network it is supplying. In the event of a network failure outside of Ofilms brief Ofilms will not be held responsible
2. Ofilms uses a number of suppliers to deliver internet connections. These have a variety of SLAs should a supplier fail to deliver the SLA Ofilms will do its best to recover monies from the supplier and pass 100% of these to the customer. However even in the event of a complete supplier failure all other equipment and services must be paid for even if the supplier refuses compensation
3. Should a failure occur a reasonable time must be allowed for correction.

ISP CHARGES

1. ISP costs are always payable regardless of cancellation time. If any amount to be paid to Ofilms is not paid in full, or properly credited by the payment date, then the customer shall also be liable for interest on the unpaid amount for the period beginning on the Payment Date and ending on the date that the amount is settled in full. The amount of interest to be paid shall be computed using an annual rate equal to 4% percent above the Bank of England base rate

GDPR

1 **Definitions**

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement the definitions in the standard terms:

Agreed Purposes	has the meaning given to it in sub-paragraph 2.3 (Status of the Parties)
Business Contact Details	first and last name, business telephone number, email address, office location and position/job title and/or role
Claim Losses	has the meaning given to it in paragraph 7.3 (Liabilities of Data Protection Breach) of Annex 2 (Joint Controller Agreement) to this Schedule
Data Loss Event	means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	an assessment by the Controller carried out in accordance with section 3 of the UK GDPR and sections 64 and 65 of the DPA 2018
Data Protection Officer	has the meaning given to it in the UK GDPR
Data Subject Request	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data
Financial Penalties	has the meaning given to it in paragraph 7.1 (Liabilities of Data Protection Breach) of Annex 2 (Joint Controller Agreement) to this Schedule
Joint Control	where two or more Controllers jointly determine the purposes and means of Processing
Lead Controller	has the meaning given to it in paragraph 1.2 (Joint Controller status and allocation of responsibilities) of Annex 2 (Joint Controller Agreement) to this Schedule
Personnel	all directors, officers, employees, agents, consultants and contractors of a Party engaged in the performance of its obligations under this Agreement
Processor Personnel	all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Subprocessor engaged in the performance of its obligations under this Agreement
Protective Measures	appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Agreement, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it
Subprocessor	any third party appointed to process Personal Data on behalf of the Processor related to this Agreement
Supplier	Means Ofilms, and its Personnel.

2. **Status of the Parties**

2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under this Agreement dictates the status of each Party under the DPA 2018. A Party may act as:

2.1.1 **"Controller"** in respect of the other Party who is "Processor";

2.1.2 **"Processor"** in respect of the other Party who is "Controller";

2.1.3 **"Joint Controller"** with the other Party;

2.1.4 **"Independent Controller"** of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under this Agreement and will specify in Annex 1 (Processing Personal Data) of this Schedule which scenario they think will apply in each situation.

2.2 Each Party must comply with its respective legal obligations under the Data Protection Legislation in accordance with the role it is performing under this Agreement and allow the other Party to comply with its obligations by providing them with all necessary information.

2.3 The Parties must Process the Personal Data for the purposes of fulfilling their obligations under this Agreement and pursuant to the terms of this Schedule or in order to comply with an obligation imposed upon them under applicable Law (the "**Agreed Purposes**").

3. **Where one Party is Controller and the other Party its Processor**

3.1 Where a Party is a Processor, the only Processing that it is authorised to do is listed in the applicable table in Annex 1 (Processing Personal Data) by the Controller and may not be determined by the Processor.

3.2 The Processor must notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

3.3 The Processor must, at the Processor's cost, provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing and must continue to provide reasonable assistance to the Controller to ensure that any such Data Protection Impact Assessment is maintained throughout the duration of this Agreement. Such assistance may, at the discretion of the Controller, include:

3.3.1 a systematic description of the envisaged Processing and the purpose of the Processing;

3.3.2 an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

3.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

3.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

3.4 The Processor must, in relation to any Personal Data Processed in connection with its obligations under this Agreement:

3.4.1 Process that Personal Data only in accordance with Annex 1 (Processing Personal Data), unless the Processor is required to do otherwise by Law. If it is so required the Processor must promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

3.4.2 notwithstanding any other provisions in this Agreement relating to (amongst others) security, ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject will not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

a) nature of the data to be protected;

b) harm that might result from a Data Loss Event;

c) state of technological development; and

d) cost of implementing any measures;

3.4.3 ensure that:

a) the Processor Personnel do not Process Personal Data except in accordance with this Agreement (and in particular Annex 1 (Processing Personal Data));

b) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this Schedule;

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

3.4.4 not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the destination country has been recognised as adequate by the UK Government in accordance with Article 45 of the UK GDPR or section 74 of the DPA 2018;

b) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or section 75 of the DPA 2018) as determined by the Controller;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and/or

e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

3.4.5 at the written direction of the Controller, securely delete or return Personal Data (and any copies of it) to the Controller on termination or expiry of this Agreement, unless the Processor is required by Law to retain the Personal Data.

3.5 Subject to paragraph 3.6 of this Schedule, the Processor must notify the Controller immediately if, in relation to Processing Personal Data under or in connection with this Agreement, it:

3.5.1 receives a Data Subject Request (or purported Data Subject Request);

3.5.2 receives a request to rectify, block or erase any Personal Data;

3.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

3.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Agreement;

3.5.5 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

3.5.6 becomes aware of a Data Loss Event.

3.6 The Processor's obligation to notify under paragraph 3.5 of this Schedule includes the provision of further information to the Controller, as details become available.

3.7 Taking into account the nature of the Processing, the Processor must (at its own expense) provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 3.5 of this Schedule (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

3.7.1 the Controller with full details and copies of the complaint, communication or request;

3.7.2 such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

3.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

3.7.4 assistance as requested by the Controller following any Data Loss Event; and/or

3.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's or any other regulatory authority.

3.8 The Processor must maintain complete and accurate records and information to demonstrate its compliance with this Schedule. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

3.8.1 the Controller determines that the Processing is not occasional;

3.8.2 the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

3.8.3 the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

3.9 The Processor must allow for audits of its Processing activity by the Controller or the Controller's designated auditor.

3.10 Each Party must designate its own Data Protection Officer if required by the Data Protection Legislation.

3.11 Before allowing any Subprocessor to Process any Personal Data related to this Agreement, the Processor must:

3.11.1 notify the Controller in writing of the intended Subprocessor and Processing;

3.11.2 obtain the written consent of the Controller;

3.11.3 enter into a written agreement with the Subprocessor which gives effect to the terms set out in this Schedule such that they apply to the Subprocessor; and

3.11.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

3.12 The Processor remains fully liable for all acts or omissions of any of its Subprocessors and the Processor must cease to engage a Subprocessor appointed pursuant to paragraph 3.11 upon the Controller's withdrawal of consent where it has reasonable grounds for doing so including where the Controller has concerns regarding the Subprocessor's ability to Process the Personal Data in a manner contemplated by this paragraph 3.

3.13 The CMA may, at any time on not less than thirty (30) Working Days' notice, revise this Schedule by replacing it with any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

3.14 The Parties agree to take account of any guidance issued by the Information Commissioner. The CMA may, on not less than 30 Working Days' notice to the Consultant, amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner.

4. **Where the Parties are Joint Controllers of Personal Data**

4.1 In the event that the Parties are Joint Controllers in respect of Personal Data under this Agreement, the terms set out in Annex 2 (Joint Controller Agreement) shall apply in respect of such Processing. The Parties must only provide Personal Data to each other as Joint Controllers where it is recorded in the applicable table under Annex 1 (Processing Personal Data).

5. **Where the Parties are Independent Controllers of Personal Data**

5.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as an Independent Controller.

5.2 Each Party must Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

5.3 Where a Party has provided Personal Data to the other Party in accordance with paragraph 5.1 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

5.4 The Parties will be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of this Agreement.

5.5 The Parties must only provide Personal Data to each other:

5.5.1 to the extent necessary to perform their respective obligations under this Agreement;

5.5.2 in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

5.5.3 where it is recorded in the applicable table in Annex 1 (Processing Personal Data).

5.6 Subject to paragraph 5.5, the Party receiving Personal Data must not transfer that Personal Data to a third party located outside of the UK unless:

5.6.1 it has obtained the prior written consent of the other Party; and

5.6.2 such transfer is necessary to achieve the Agreed Purposes, protected with appropriate supplementary measures and complies with the transfer restrictions set out under Chapter V of the UK GDPR.

5.7 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party must, with respect to its Processing of Personal Data as Independent Controller, implement and maintain Protective Measures to ensure a level of security appropriate to that risk. The measures must, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

5.8 A Party Processing Personal Data for the purposes of this Agreement must maintain a record of its Processing activities in accordance with Article 30 of the UK GDPR and must make the record available to the other Party upon reasonable request.

5.9 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to this Agreement (**"Request Recipient"**):

5.9.1 the other Party must provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

5.9.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

a) promptly, and in any event within 5 Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

b) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

5.10 Each Party must promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to this Agreement and must:

5.10.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

5.10.2 implement any measures necessary to restore the security of any compromised Personal Data;

5.10.3 work with the other Party to make any required notifications to the Information Commissioner or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

5.10.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

5.11 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under this Agreement as specified in Annex 1 (Processing Personal Data).

5.12 Personal Data must not be retained or processed for longer than is necessary to perform each Party's respective obligations under this Agreement which is specified in Annex 1 (Processing Personal Data).

Notwithstanding the general application of paragraphs 3.1 to 3.14 (Where one Party is a Controller and the other Party is a Processor) of this Schedule to Personal Data, where the Consultant is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of that Personal Data in accordance with paragraphs 5.1 to 5.12 of this Schedule.

Annex 1
Processing Personal Data

1. This Annex will be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex will be with the CMA at its absolute discretion.

2. The contact details of the CMA's Data Protection Officer are: [redacted]

3. The contact details of the Consultant's Data Protection Officer are [redacted]

4. The Processor must comply with any further written instructions with respect to Processing by the Controller. Any such further instructions will be incorporated into this Annex.

Table 1: The CMA is the Controller and the Consultant is the Processor

Description	Details
Category of Personal Data where the CMA is the Controller and the Consultant is the Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the CMA is the Controller and the Consultant is the Processor of the following Personal Data: Written, digital, electronic or Audio or Video (inclusive of spoken) Data.
Duration of the Processing	For the duration of the contract.
Nature and purposes and subject matter of the Processing	The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose is to enable the Authority to conduct its statutory obligation to protect consumers.
Type of Personal Data	Name, address, telephone number, images inclusive of video.
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.
International transfers and legal gateway	Personal data may geographically stored or accessed from the UK or EEA only. (The UK Government has declared that the European Union and European Economic Area are adequate for data protection purposes. Likewise the European Commission has also declared that the UK is adequate for data protection purposes. This means that personal data can flow unfettered between the UK and the EU/EEA. For the performance of this contract). Outside of UK and the EU/EEA or Geographical Jurisdictions where and adequacy decision is not in place international transfers will be governed by an International Data Transfer Agreement between the Controller and Processor or Sub-processor.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Law to preserve that type of data	All personal Data should be returned and / or securely destroyed upon termination of the contract.
Protective Measures that the Consultant and, where applicable, its Sub-contractors have implemented to protect Personal Data Processed under this Agreement against a breach of security (insofar as that breach of security relates	Risk Assessment The Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address risks involved in processing the CMA's data in the performance of the Contract.

to data) or a Data Loss Event	

PAYMENT

1. Ofilms will normally require 100% payment upfront unless credit or part payment has been agreed, in this instance invoices must be sent to the CMA Accounts Payable at the following email address [redacted] 50% will be paid at least 2 days before the first day on site and the balance will be will be invoiced in arrears with 28 day terms.
2. Cancellation payments are
    1. Up to 14 days before 1st rig day – 45% charge
    2. Under 3 days to first rig day – full charge
    3. ISP and digital delegate costs are always payable regardless of cancellation time

[redacted]

Signature Date