

MIA Call-Off Agreement

1	Supplier name	
2	Supplier address (including post code)	
3	Contact name	
4	Contact email	
5	Telephone number	
6	Company registration number	
7	Delivery date	(of the Equipment to the Authority)
8	Authority	
9	Authority address (including post code)	
10	Authority contact name	
11	Authority contact email	
12	Authority telephone number	
13	Type of Equipment and its purpose	
14	Model and make	
15	Serial numbers	
16	Value	
17	Personal Data and Data Subjects	<p>Will the MIA Call-Off Agreement involve the Processing of Personal Data? [Please enter "yes" or "no" as appropriate]</p> <p>If yes, Schedule 1 - Information Governance and System Security of the MIA Terms and Conditions shall apply and the Data Protection Protocol (appended below) must be completed by the parties and used</p>
18	IT systems and Security of IT systems	<p>The Authority's IT systems are used to provide essential services</p> <p>If the Equipment is used for the purposes of any essential services or together with any of the</p>

v1.01

		Authority's IT systems, the extent of this should be detailed here: [enter text as appropriate]
19	Timescales for request to audit for compliance with Data Protection Legislation and Security of IT Systems	[Insert agreed notice period if different to 4 week notice period as set in paragraph 3.10 of the Schedule to the MIA Terms and Conditions]
20	Loan or transfer?	[Please note that where disposable Equipment is provided, this should only be on a transfer basis]
21	Purpose of loan or transfer	
22	Loan time period	[Complete only where the Equipment is to be loaned, not transferred] [Please state number of days, months or years and the date of commencement]
23	Premises and locations at which the Equipment will be kept (including post codes)	
24	In consideration of the Authority taking the Equipment on a loan or transfer basis for the purposes outlined above MIA Indemnity Agreement Terms and Conditions, the Authority and the Supplier confirm that the MIA Terms and Conditions shall apply to the provision of the above Equipment by the Supplier to the Authority (on either a loan or transfer basis as specified above) and that upon signature of this MIA Call-Off Agreement by both the Authority and the Supplier a legally binding agreement on such terms shall come into full force and effect between the parties incorporating such MIA Terms and Conditions. For the avoidance of doubt the MIA Terms and Conditions and any updates are published on the Master Indemnity Agreement website - https://www.supplychain.nhs.uk/mia	

Signed on behalf of the Supplier	
Name and position of signatory	
Date	
Signed on behalf of the Authority	
Name and position of signatory	
Date	

Collection Confirmation Receipt - for Equipment on loan only

To be completed at the point that the Equipment is collected by the Supplier.

Without prejudice to the Authority's rights under this MIA Call-Off Agreement in relation to any outstanding obligations and / or liabilities of the Supplier, the Authority confirms collection by the Supplier, and the Supplier confirms it has checked the Equipment and it [has been appropriately decontaminated and] [also all Personal Data has been removed], [and following such checks now confirms] receipt, of the Equipment detailed below.

Type of Equipment and its purpose	
Model and make	
Serial numbers	
Date of collection	
Signed on behalf of the Authority	
Name and position of signatory	
Date	
Signed on behalf of the Supplier	
Name and position of signatory	
Date	

Data Protection Protocol

This Data Protection Protocol is to be used alongside the MIA Terms and Conditions where the Supplier will be processing personal data on behalf of the Authority. In these circumstances, the table below should be completed by the Authority setting out the nature of the processing that will be taking place under this MIA Call-Off Agreement.

Table A shall be completed by the Authority, who may take account of the view of the Supplier, however the final decision as to the content of Table A shall be with the Authority at its absolute discretion.

1. The contact details of the Authority's Data Protection Officer are:

[Insert contact details]

2. The contact details of the Supplier's Data Protection Officer are:

[Insert contact details]

Table A - Processing, Personal Data and Data Subjects	
Description	Details
Identity of the Controller and Processor	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor in accordance with Clause 1.1 of this Data Protection Protocol.</p> <p>[You may need to vary this section where (in the rare case) the Authority and Supplier have a different relationship. For example where the Parties are Joint Controller of some Personal Data: "Notwithstanding Clause 1.1 of this Data Protection Protocol the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of: [insert the scope of Personal Data which the purposes and means of the Processing is determined by both Parties]</p> <p>In respect of Personal Data under Joint Control, Clause 1.1 - 1.15 of this Data Protection Protocol will not apply and the Parties agree to put in place a Joint Controller Agreement instead."]</p>
Subject matter of the Processing	<p>[This should be a high level, short description of what the Processing is about i.e. the subject matter of the contract.</p> <p>Example: The Processing is needed in order to ensure that the Processor can effectively deliver the MIA Call-Off Agreement and enable the Authority to use the Equipment to provide a service to members of the public.]</p>

v1.01

Duration of the Processing	[Clearly set out the duration of the Processing including dates]
Nature and purposes of the Processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p>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.</p> <p>The purpose might include employment processing, statutory obligation, recruitment assessment etc.]</p>
Type of Personal Data being Processed	[Examples include name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]
Special Categories of Personal Data being Processed	<p>[Special categories of personal data under Article 9 of the UK GDPR include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. In addition, criminal convictions under Article 10 of the UK GDPR should be treated in a similar manner.</p> <p>Special categories of Personal Data require restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.]</p>
Categories of Data Subject	[Examples include Staff (including volunteers, agents, and temporary workers), customers / clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]
Plan for the return and destruction of the data once the Processing is complete unless requirement under union or member state law to preserve that type of data	[Describe how long the data will be retained for, how it will be returned or destroyed after use]

v1.01

Definitions

The definitions and interpretative provisions at Clause 1 (Definitions) and Schedule 1 (Information Governance and System Security Provisions) of the MIA Terms and Conditions shall also apply to this Protocol.

Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
“Data Subject Access Request”	means 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.
“International Data Transfer Agreement”	the Information Commissioner's Office International Data Transfer Agreement for use with the transfer of Personal Data from the UK to processors established in third countries, as set out at https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx ;

<p>“Protective Measures”</p>	<p>means such appropriate technical and organisational measures which ensure a level of security appropriate to the risk involved while taking account of the harm that may result from a Data Loss Event, the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.</p> <p>Protective Measures may include (as appropriate):</p> <ul style="list-style-type: none"> (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to ensure that availability of and access to Personal Data can be restored in a timely manner in the event of an incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of such measures adopted by the Supplier;
<p>“Protocol” or “Data Protection Protocol”</p>	<p>means this Data Protection Protocol;</p>
<p>“Sub-processor”</p>	<p>means any third party appointed to Process Personal Data on behalf of the Supplier related to this MIA Call-Off Agreement.</p>

DATA PROTECTION

- 1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.
- 1.2 The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

Data Protection Impact Assessment

v1.01

1.3 The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, include:

1.3.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

1.3.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Supplier's obligations under this MIA Call-Off Agreement;

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

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

Specific Data Processing Obligations

1.4 The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this MIA Call-Off Agreement:

1.4.1 process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by **Law**. **If it is so required, the Supplier** shall promptly notify the Authority before Processing the Personal Data unless such notification is prohibited by Law;

1.4.2 ensure that, at all times, it has in place Protective Measures to protect against a Data Loss Event, against accidental, unauthorised or unlawful Processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data;

1.4.3 ensure that:

(i) the Staff do not Process Personal Data except in accordance with this Contract (and in particular Table A of this Protocol);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this Protocol;

v1.01

- (B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
- (C) 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 Authority or as otherwise permitted by this MIA Call-Off Agreement; and
- (D) have undergone adequate training in the use, care, protection and handling of Personal Data;

International Transfers

1.4.4 not transfer or otherwise Process Personal Data outside of the UK unless the prior written consent of the Authority has been obtained. Without prejudice to the foregoing, the Supplier must not transfer or otherwise Process Personal Data outside the UK unless it ensures that one or more of the following conditions are fulfilled:

- (i) the transfer is to a country approved under the applicable Data Protection Legislation as providing adequate protection (via an adequacy decision or adequacy regulation);
- (ii) the Authority or the Supplier has provided appropriate safeguards or binding corporate rules in relation to the transfer, pursuant to the applicable Data Protection Legislation, as determined by the Authority;
- (iii) the Supplier otherwise 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 Authority in meeting its obligations); or
- (iv) one of the derogations for specific situations in the applicable Data Protection Legislation applies;

1.4.5 ensure that, whenever the Supplier transfers or otherwise Processes Personal Data outside of the UK, it ensures that:

- (i) the Data Subject has enforceable rights and effective legal remedies; and
- (ii) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;

1.4.6 without prejudice to the conditions set out in this Protocol and unless it can demonstrate that one or more of the protections set out under clause 1.4.4 are otherwise met, put in place the

v1.01

International Data Transfer Agreement with each of the relevant Sub-processors prior to any transfers of Personal Data outside of the UK, and to promptly provide a validly executed copy of the same to the Authority on written request.

Deletion or Return of Personal Data

- 1.4.7 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of this MIA Call-Off Agreement unless the Supplier is required by Law to retain the Personal Data.

Notifications

- 1.5 Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if, in relation to any Personal Data Processed in connection with its obligations under this MIA Call-Off Agreement, it:
- 1.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 1.5.2 receives a request to rectify, block or erase any Personal Data;
 - 1.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this MIA Call-Off Agreement;
 - 1.5.5 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
 - 1.5.6 becomes aware of a Data Loss Event.
- 1.6 The Supplier's obligation to notify under Clause 1.5 of this Protocol shall include an obligation to provide further information to the Authority in phases, as details become available.
- 1.7 The Supplier must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Authority's written instructions, or as required by Law.
- 1.8 Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either party's obligations under Data Protection Legislation in

v1.01

relation to any Personal Data Processed in connection with its obligations under this MIA Call-Off Agreement and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

- 1.8.1 the Authority with full details and copies of the complaint, communication or request;
- 1.8.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
- 1.8.3 the Authority, at its request, with any Personal Data it holds in connection with its obligations under this MIA Call-Off Agreement in relation to a Data Subject;
- 1.8.4 assistance as requested by the Authority following any Data Loss Event;
- 1.8.5 assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.

Records, Compliance & Audit

- 1.9 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
 - 1.9.1 the Authority determines that the Processing is not occasional;
 - 1.9.2 the Authority determines the Processing includes Special Categories of Personal 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
 - 1.9.3 the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 1.10 The Supplier shall allow for audits of its Processing activity by the Authority or the Authority's designated auditor in relation to any Personal Data Processed in connection with its obligations under this MIA Call-Off Agreement.

v1.01

1.11 The Supplier shall contribute to and give the Authority and its third party representatives all necessary assistance to conduct such audits at no additional cost to the Authority.

1.12 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

Use of Sub-Processors

1.13 Before allowing any Sub-processor to Process any Personal Data related to this MIA Call-Off Agreement, the Supplier must:

1.13.1 notify the Authority in writing of the intended Sub-processor and Processing;

1.13.2 obtain the written consent of the Authority;

1.13.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and

1.13.4 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

1.14 Any intended changes or additions to, or replacement of, Sub-processors must be notified in writing to the Authority by the Supplier and the written consent of the Authority must be obtained.

1.15 The Supplier shall remain fully liable for all acts or omissions of any Sub-processors.

Variations

1.16 The Authority may, at any time on not less than 30 Business Days' notice, revise this Protocol 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 MIA Call-Off Agreement).

1.17 The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A above from the date at which such notice is treated as having been received by the Supplier in accordance with clause 14.9 of the MIA Terms and Conditions.

v1.01

1.18 Subject to clauses 1.16, 1.17, and 1.19 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both parties.

ICO Guidance

1.19 The parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Business Days' notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner's Office.

to be printed on the Authority's letterhead