# Off-Framework – user permissions form (EX107 OFC)

**When to use this form:**

**This form gives limited permission to prepare a transcript or report from a recording made other than by the court/tribunal, and where the court/tribunal are not contributing to the commissioning of those services.**

**Permission to use transcription services must be obtained from a Judge via completion of this form. *By exception, if permission is given verbally in the court/tribunal this form must be completed retrospectively and submitted to the court/tribunal for formal approval*.**

**The applicant must complete part 1 of this form, sections A and B, and it should then be passed to the member of the judiciary conducting the hearing. Once approval has been granted, the court should complete section C and this should be retained by the Judge's Clerk.**

## Part 1: For completion by requestor

### A. APPLICANT / REQUESTOR AND REQUIREMENT FOR TRANSCRIPT

| | |
|---|---|
| Name/address/email of applicant(s) (e.g. parties in the action): | |
| Your involvement in the case: | |
| Intended use of transcript: | |
| Details of any third party on whose behalf the transcript is to be prepared or any third party to whom the transcript will be provided | |
| Transcription supplier to be used: | |

### B. HEARING DETAILS

| | |
|---|---|
| Court/Tribunal Name: | |
| Court/Tribunal Postal Address of hearing site: | |
| Court/Tribunal Hearing Room Number: | |
| Court/Tribunal Case Reference: | |
| Judge's Name: | |
| Date of Hearing: | |
| Reporting Restrictions imposed: | |
| Security marking allocated to the case (if known): | ☐ **None** ☐ **Official** ☐ **Official Sensitive** ☐ **Secret** |

**C. For internal use: JUDICIAL APPROVAL**

**Approved:** **Yes:** ☐

**No:** ☐

**Name and title of approver:**

**Date:**

**Once permission has been granted, the supplier must liaise with the court to confirm the following information:**

- **When they will attend the court to set up any necessary equipment in advance of the hearing. At the same time, the timeframes for the disassembling of any equipment must be agreed;**
- **Named contact for them to report to at the court;**
- **Whether the transcript needs to be approved by the judge before it can be finalised; and**
- **Details of where the transcript for approval must be sent.**

**Part 2, section D of this form must read by the transcription supplier and the declaration signed at section E. This should also be retained by the Judge's Clerk.**

## Part 2: For completion by approved transcription supplier

### D. TERMS AND CONDITIONS APPLYING TO THE TRANSCRIPTION PROVIDER FOR PERMITTED TRANSCRIPTS AND REPORTS

In consideration for the Crown granting permission to the transcription provider to take a transcript or prepare a report in respect of the above hearing, you, the transcription provider, agree that the following provisions shall apply in respect of such transcript or report:

1. Court judgments and tribunal reports are protected by Crown copyright. Therefore, if and to the extent that any intellectual property rights are created (**Created IPR**) in the transcript or report you hereby assign to the Authority, with full title guarantee, title to and all present and future rights and interest in such rights or shall procure that the owner of such Created IPR assigns them to the Authority on the same basis.

2. If requested by the Authority, you shall, without charge to the Authority, execute all documents and do all such acts as the Authority may require to perfect the assignment of Created IPR under paragraph 1, or shall procure that the owner of such rights does so on the same basis.

3. The Authority grants to you and to any third party specified in Part A above a limited, non-exclusive, non-assignable licence (with no right to sub-license) to use the transcript you prepare

strictly for the intended use indicated above. In particular (and notwithstanding any description of the intended use provided), you may not:

3.1 make publicly available (either by itself or as part of any other material);

3.2 provide to a third party not specified above;

3.3 otherwise publish (whether or not for payment of a

fee) the whole or any part of the transcript.

4. You shall comply with any and all security markings stated in Box B above or as they become relevant to the hearing.

5. You shall provide a copy of the transcript or report you prepare, to the court at which the hearing takes place.

**6. The use of Hand Held audio equipment is permitted for use in the production of the Transcript(s) in this case only.**

7. In preparing the transcript or report, you shall comply with the information security requirements in Annex 1.

8. You shall obtain judicial sign off of any judgment before it is released to any party unless the judge specifically states it is not required.

**E. DECLARATION BY TRANSCRIPTION PROVIDER**

I agree to comply with the terms and conditions above in connection with the transcript/report of the hearing noted above.

NAME AND ADDRESS OF TRANSCRIPTION PROVIDER

**Auscript Ltd**
Central Court
25 Southampton Buildings
London, WC2A 1AL
DX 82 Chancery Lane
uk.clientservices@auscript.com
+44 (0)3301 005223

**Signature**

**Date:**

**ANNEX 1**

**Information Assurance**

## 1. SECURITY CLASSIFICATIONS DEFINITIONS

1.1. You shall abide by the following Government Security Classifications.

1.2. There are 3 security classifications (OFFICIAL, SECRET and TOP SECRET) indicate the increasing sensitivity of information AND the baseline personnel, physical and information security controls (see 2.2.5) necessary to defend against a broad profile of applicable threats. Additionally, there is a classification that refers to a limited amount of information which will be particularly sensitive but will still come under the OFFICIAL marking even if its loss or compromise could have severely damaging consequences. This more sensitive information will be identified by adding 'SENSITIVE' and must therefore be marked 'OFFICIAL-SENSITIVE':

### 1.2.1. OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

### 1.2.2. OFFICIAL-SENSITIVE

This marking alerts Users to the enhanced level of risk and that additional controls are required. The need to know principle must be rigorously enforced for this information particularly where it may be being shared outside of a routine or well understood business process

### 1.2.3. SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

1.2.4. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. As a minimum, all HMG information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. There is no requirement to mark routine OFFICIAL information.

## 2. TRANSMISSION OF INFORMATION

2.1. Transcription suppliers shall take reasonable steps in all cases to ensure secure transmission, including checking that recipient email addresses are accurate and genuine and requesting confirmation of receipt, and using read receipts as standard.

2.2. Where you facilitate your business via downloading and burning audio onto removable media for onward transmission, the Authority requires that you shall use an encrypted CD and only use secure methods of delivery, examples of which, includes Special Delivery or secure courier transfer.

2.3. You shall send all hard copy material, no matter what security classification via tracked mail using Special Delivery (or equivalent service) and double enveloping of the contents. The inner envelope should have the relevant security marking on it. The security marking MUST NOT be placed on the outer envelope, rather it should be marked "Addressee only".

**General Guidance to be applied by Transcribers using their own IT devices to process MoJ /HMCTS information.**

This Guidance was originally drafted for Transcribers but for the purposes of this contract will also apply to Suppliers and their personnel.

1. ***Set a password on the device - MANDATORY***
   It is important to add one as if the device is misplaced or stolen it will make it harder for someone to gain access to the device and any information on it.
2. ***Set a timeout lock on the device - MANDATORY***
   If the device were to be stolen whilst logged in, this will add some protection in minimising the time the device would be accessible (15 minutes or ideally a shorter time).
3. ***Keep all software up to date – MANDATORY***
   There are features that run locally (e.g. One Drive) which may create a connection to the internet. When services complete upgrades to their products they assume the latest (or no older than one version) products are in use. This will also allow support to be maintained and to be provided more cost effectively and consistently, and ensures that the device runs correctly.
4. ***Install and enable anti-virus and anti-spyware – MANDATORY***
   This is necessary to prevent malicious software gaining access to any information or corrupting or stealing data.
5. ***Enable a firewall (Windows device) – MANDATORY***
   This will also assist in protecting the device from malicious software.
6. ***Use a non-Administrative Account for day to day work – MANDATORY***
   If an unauthorised user were to gain access to your device this limits the amount of access and control they would have over the device.
7. ***Only install trusted software from a trusted site - RECOMMENDED***
   This is difficult to define accurately and hence the recommendation status. Untrusted software, will of course, increase the potential at best for unwanted/requested software to be installed and at worse malicious software.

IMPORTANT NOTE: If the device you are using does not comply with the above mandatory requirements, then do not use the device