

Application for permission to prepare a transcript or report from a recording made other than by the court

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.*

Part A - Applicant and requirement for transcript

A1. Applicant's name (Solicitor's firm or applicant in person)

A2. Applicant's address

Postcode

--	--	--	--	--	--	--	--

A3. Email

A4. What is your involvement in the case?

A5. What is your intended use of the transcript?

A6. Give 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

Part B - Hearing details

B1. Name of Court or Tribunal where proceedings/hearing are taking place/took place

B2. Court or Tribunal address

Postcode

B3. Court or Tribunal Case reference number

B4. Name of judge

B5. Date(s) of hearing

Start date

B6. Have reporting restrictions been imposed?

- Yes
 No
 Don't know

B7. What security marking has been allocated to the case?

- None
 Official
 Official Sensitive
 Secret

B8. If applicable, give name of other Government Department requesting permission (Crown Authority)

C. Terms and conditions applying to the transcription provider for permitted transcripts and reports

In consideration for the Crown granting permission to the transcription provider 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 Crown, 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 Crown on the same basis.
2. If requested by the Crown, you shall, without charge to the Crown, 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 Crown 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 security markings stated in Box B above or as they become relevant to the hearing.
5. The following reporting restrictions shall apply

and or any that become relevant during the hearing.

6. You shall provide a copy of the transcript or report you prepare, to the court at which the hearing takes place.
7. The use of hand held and audio recording equipment is prohibited. Any requests to use hand held equipment should be made to HMCTS.
8. In preparing the transcript or report, you shall comply with the information security requirements in Annex 1.

9. You shall obtain judicial sign off of any transcript before it is released to any party including those who are requesting it unless the judge specifically states it is not required.
10. If the judge approves publication of the transcription, or any part thereof, you shall provide a copy of the transcript to the following authorised publishers:

Justis Publishing - Masoud Gerami - Masoud.gerami@justis.com

Thomson Reuters - Ian Law - ian.law@tr.com

- Sarah Edwards - sarah.edwardes@thomsonreuters.com

ICLR - Daniel Hoadley - Daniel.hoadley@iclr.com

LexisNexis - Kirstyn Forward - caselaw@lexisnexis.co.uk

D. 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 Central Court 25 Southampton Buildings London WC2A 1AL

Signature

Auscript

Date

--

E. Crown/Other Government Department approval

Approved

Yes

No

Name and title of approver

--

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 within 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. Contractors 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 facilitates 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 worst malicious software.

IMPORTANT

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