Recording and Transcription Policy

1. Introduction and Purpose

1.1 Royal Holloway subscribes to sound corporate governance principles, one of which is the use and application of Policies and Governance Standards which define and articulate practices, boundaries, and expectations within which the College will operate.

1.2 The purpose of the Recording and Transcription Policy is to ensure that the College’s IT supported information and communications technologies (ICT) are used appropriately to create and manage records that document spoken words through audio/video recording or automated transcription.

2. Terminology

2.1 Automated speech recognition (ASR) is the automatic transcription of speech into text using automated technologies. ASR is undertaken by computers and cannot be guaranteed to be accurate. For example, the text displayed may be erroneous, or the text may be attributed to the wrong speaker. Accuracy will be lower if technical or niche terms (jargon) are used. Accuracy will also suffer if the speaker talks too fast, is talking from a noisy environment, or if more than one person talks at once.

2.2 Live captioning is the use of a manual captioning service or ASR to generate subtitles for live video. The transcribed text will appear as on-screen subtitles, attributed to the speaker but is not saved.

2.3 Recording is saving meeting video and/or audio as a stored media file so that it can be replayed.

2.4 Transcription is the use of a manual transcription service or ASR to convert spoken words into written text and saving as a stored document (a transcript).

3. Scope

3.1 This policy covers the use of automated audio/video recording and transcription functionality provided by the College’s IT supported information and communications technologies (ICT).

3.2 IT supported technologies should be used for automated recording and transcription as these have been assured as safe and secure and fit for purpose, reducing information security risks.

3.3 IT supported automated recording and transcription technologies are:

3.3.1. **Microsoft Teams** is the recommended technology for meeting recording and transcription and is the only IT supported video conferencing platform.

3.3.2. **Panopto** is the recommended technology for teaching and learning and is the only IT supported lecture recording platform.

4. Policy Statement

4.1 The use of recording and transcription features of IT supported technologies is permitted but users should be mindful that recording and transcription creates fully searchable records of spoken conversations and so should think carefully about the sensitivity of the discussion and whether the use automated recording/transcription is appropriate.

4.2 We have obligations to comply with security, privacy, and relevant statutes and regulatory frameworks such as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018, and the Freedom of Information Act (FOIA) 2000. When using recording and transcription it is safest to assume that all such recordings will be subject to these regulations and recordings/transcripts may be subject to Data Subject Access (DSA) and Freedom of Information (FOI) requests.

4.3 Live captions can be used at any time as an accessibility aid.

4.4 Consent should be sought from participants before using recording/transcription.

4.5 If the intention is to use recording/transcription for an external event, this should be included in the privacy notice for the event.

4.6 Participants should be clearly notified via an audible and visual indicator when recording/transcription starts and stops.

4.7 Participants should be advised how they can participate anonymously should they not wish to be identified.
4.8 Participants should generally be given an opportunity to review, edit, or erase any audio or video recording to which they have contributed. If this is impractical, as with group recordings, individuals should be given an opportunity to review, edit, or erase their contribution on a written transcript of the recording.

4.9 Automatically generated transcripts should be checked for quality, and any errors or unwanted sections corrected, as soon as possible.

4.10 Recordings and transcripts should not be kept indefinitely and should be deleted when no longer required. This should be within 30 days or as defined by an approved retention policy or data management plan.

4.11 Recordings/transcripts should be stored in a secured location. It is recommended that IT support storage technologies such as Microsoft 365 or shared drives are used. Any non-IT supported storage location should offer an equivalent level of security and assurance. Transfer of recordings/transcripts between storage locations should be done securely, via an encrypted connection or device.

4.12 Access to recordings/transcripts should be controlled and limited to a defined audience.

4.13 Recordings/transcripts should be shared via cloud sharing links rather than by distributing copies. By default, downloading of this file should not be permitted but should be viewed online.

4.14 Recordings/transcripts should only be downloaded to encrypted devices such as College managed PCs. All files should be deleted from devices when no longer required for local processing.

5. Microsoft Teams

5.1 The ability to record and/or transcribe a meeting is granted in Teams via meeting policies. Whether a user has these features enabled depends on the policy that is assigned to them.

5.2 By default, the use recording/transcription is only available for staff accounts.

5.3 Students can be temporarily assigned to a policy that enables recording and/or transcription if required. Such access should be requested by a supervising member of staff via the IT Service Desk.

5.4 Recording and transcription are started and stopped manually in Teams via an option in the Teams meeting menu.

5.5 The option to start recording automatically when the meeting is started should not be used because of the need to obtain consent and ensure appropriate ownership of the generated recording/transcript files.

5.6 Individuals can use their Teams settings to control whether they want their name to be attributed to their comments or not. However, this doesn't guarantee anonymity as they could be identified from the transcript content.

5.7 By default, external participants are not provided with access to Teams recordings/transcripts. Should they need to review, then access can be provided to them via a sharing link associated with their e-mail address.

6. Roles and Responsibilities

6.1 Compliance with this policy is mandatory for all users of Royal Holloway Information Technology resources.

6.2 Meeting organisers are accountable for the use of recording/transcription in a meeting and all recordings/transcripts generated.

6.3 The person who initiates recording (and any meeting organiser if different) are jointly responsible for obtaining consent, and ensuring recordings/transcripts are accurate, classified appropriately, stored and shared securely, and are deleted promptly.

6.4 It is the responsibility of all participants who have access to a recording/transcription to ensure any recording/transcription is protected as an information asset and is not shared with parties who are not authorised for that information.

7. Related Documents

7.1 Acceptable use of Information Technology
7.2 Information Security Policy
7.3 Data Protection Policy
7.4 Records Retention Policy and Schedule
7.5 Lecture Recording Policy
7.6 Codes of Good Research Practice
7.7 Research Data Management Policy
7.8 Research Ethics Policy / Guidance Notes
7.9 Intellectual Property Policy
8. Monitoring and Compliance

8.1 The IT Services Department is responsible for the implementation of this policy and may enlist other departments to assist in the monitoring and maintenance of compliance with this policy.

8.2 Any inquiries or comments regarding this policy shall be submitted to the IT Services Team by sending an email to ITServiceDesk@rhul.ac.uk.

9. Document Control Information

<table>
<thead>
<tr>
<th>Policy Owner (usually Director-level)</th>
<th>Chief Information Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approving Body</td>
<td>Executive Board</td>
</tr>
<tr>
<td>Approved on</td>
<td>07/12/2021</td>
</tr>
<tr>
<td>To be reviewed before</td>
<td>December 2024</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version History</th>
<th>Date of approval</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version (newest to oldest)</td>
<td></td>
<td>Drafted by IT and Data Protection for submission to Information Governance Committee and Executive Board.</td>
</tr>
</tbody>
</table>