Recording of teaching, events or meetings policy

1. Introduction

1.1. It is the policy of De Montfort University (DMU) that appropriate measures are taken to ensure that all recording of electronic meetings, events or remote synchronous teaching and learning is undertaken in compliance of the legal requirements under the Data Protection Act 2018 and related regulations regarding data or personal privacy. This policy outlines the requirements which must be adhered to for the recording of such electronic meetings or other similar types of activities.

2. Scope

2.1. This policy applies to all recording of electronic meetings in DMU, irrespective of the recording mechanism.

2.2. It covers the use of systems or devices such as (but not limited to):

- Blackboard Collaborate Ultra
- MS Teams
- Zoom
- Webcams attached to recording software
- Audio recordings, including hand held recording devices such as Dictaphones or smart phones
- Other video recording applications, including video cameras, telephones & mobile phones
- PowerPoint recordings
- Panopto

Any tool used to record is covered under this policy, this list does not provide authorisation to use that tool.

2.3. It covers any electronic meeting involving DMU staff or students, or any third party acting on DMU's instruction including visiting lecturers, visiting researchers, external visitors, contractors, suppliers and agency staff.

2.4. It covers any gathering of people including teaching, learning, meetings, conferences, events, training, briefings where an electronic recording (audio or video) is taken, irrespective of the media or method used for the recording.

2.5. This policy should be considered in conjunction with other DMU policies such as DMU Replay policy on recording of staff led teaching, Data Protection, Records Management and Retention and Information Handling.

3. Definitions

3.1. **Processing** – means any operation on data, including organisation, storage, adaptation and alteration, consultation or use; disclosure, transmission, dissemination, deletion, archiving and otherwise making available.

3.2. **Electronic Meeting** – any engagement through voice and/or video between 2 or more persons

3.3. **Personal Data** – any data regarding an identifiable natural person as defined by the Information Commissioner's Office (ICO) or the Data Protection Act 2018.

4. Policy statement

4.1. No electronic meeting will be recorded by any method outside of this policy.
4.2. All recording of electronic meetings will contain some personal data and is therefore covered under the Data Protection Act 2018. As such, all use of recording will be in accordance to the seven data protection principles, and respect the privacy rights of the data subjects.

5. Implementation of Recording Policies

5.1. Recording of student teaching and learning is covered under the Student Regulations, and under the DMU Replay Policy. These should be consulted to identify permitted activity.
5.2. Recording of individual staff meetings (between manager and employee, or between tutor/academic and individual students) must not be recorded, except where this is permitted through an approved formal university policy, and where there is a full DPIA approved in advance by the Information Governance Team, and where appropriate, ratified by the Information Governance and Cyber-Security Board.
5.3. Notification of when recording is taking place will always be provided prior to a meeting commencing, and where the recording is not essential, attendees must have the opportunity to decline to be recorded, or to use an audio only recording where appropriate and agreed.
5.4. A Data Protection Impact Assessment (DPIA) will always be completed prior to any recording of an electronic meeting (see 2.4), and approved by the Information Governance Team. This may be a generic DPIA, an adjusted standard DPIA, or a DPIA for the individual recording.
5.5. All recordings of electronic meetings taken for research data gathering purposes, irrespective of the format or event being recorded will only be undertaken following ethical approval, and where a requisite and appropriate DPIA has been undertaken. This would include 1:1 meetings, face to face meetings, focus groups, electronic meetings or other similar events.
5.6. The person who arranges the recording is responsible for ensuring an approved DPIA covering the recording is completed, is accurate, and that any agreed mitigating actions are complied with.
5.7. All DPIAs regarding recording of electronic meetings will consider the following:
- 5.7.1 The lawful basis for the processing of personal data, and for any special category data
- 5.7.2 Where has the purpose of the recording been stated, and where this is available to those who are being recorded.
- 5.7.3 Arrangements agreed to ensure the recording cannot be used for other purposes
- 5.7.4 The arrangements to ensure the opportunity to object to the recording can be made, and how the situation will be managed where a participant does not wish to be recorded
- 5.7.5 How the recording will be made available, to whom, and how long will it be retained
- 5.7.6 How and when the recording will be removed/deleted (all copies)
- 5.7.7 How the recording will be secured, including any extracts.
- 5.7.8 Who will take responsibility for ensuring 5.7.1 to 5.7.7 are fully complied with
- 5.7.9 How will data subject access rights, including right of access, the right of erasure, the right to object and the right to restrict processing be exercised.
- 5.7.10 Whether the recording is proportionate with the impact on privacy rights, and what alternatives have been considered to reduce this impact

6. Consequences of non-compliance

Failure to comply with this policy could expose the university, its staff and students to risks including data breaches and legal disputes leading to reputational and financial damage to the university. The Information Commissioner can also impose a fine of up to 4% of annual turnover on the university for breaches of the Data Protection Act, and risks of enforcement action by regulators in other countries is also possible.

All personal data, including video and voice recordings, is subject to data subject access requests, and to freedom of information requests, which can be significantly burdensome to comply with.

Recordings that have been made outside of this policy introduce legal risks, and would be a breach of the staff code of conduct or the student regulations.

7. Document approval

Approved by:
Approved Date:
Review Date:
Reviewer:

8. Document history

8.1. V0.1 Draft, 5th November 2020, Jon Hill, Deputy Data Protection Officer.
8.2. V1.0, 8th November 2020, Jon Hill, Deputy Data Protection Officer