CALL RECORDING POLICY

& PROCEDURE

Policy reference	POL-357
Policy area	Data Protection
Policy owner	Kay Burton-Williams
Policy author	Seral Shevket
Level of consultation	1
Approval level	SLT
Review date	April 2025
Approval date	May 2025
Next review date	April 2026

1. Policy Statement

Birmingham Metropolitan College (BMet) is committed to ensuring the safety and security of all staff, students, apprentices, and visitors through the ethical and responsible use of call recording technology. This policy governs the ethical and responsible use of call recordings to protect individuals, property, and assets, while complying with legal obligations and respecting individual privacy.

2. Purpose

The Call Recording Policy establishes principles for the operation of call recording systems, ensuring compliance with:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

3. Key Principles

- Call recordings will be made only for legitimate purposes, including:
    - Training and quality purposes
    - Safety and security
    - The investigation of incidents
    - Protect the rights and interests of the College and individuals involved.
- The college will conduct and maintain a Data Protection Impact Assessment (DPIA) for call recording systems.
- Personal data will be processed lawfully, fairly, and transparently, and measures will be taken to protect individual privacy.
- Clear notifications will inform individuals of call recording and how to access our Privacy Notice detailing their rights.
- Regular audits will ensure compliance with this policy.

4. Scope

This policy applies to all call recording systems owned, operated, or managed by BMet, specifically for voice calls received in Contact Centre and switchboard services.

5. Governance

The Director of Student Experience is the policy owner, supported by the Student Finance and Contact Center Manager and Director of IT for implementation.

6. Call Recording Procedure

6.1 Purpose and Scope

The procedure outlines operational guidelines for managing call recording systems at BMet, ensuring safety and compliance with legal standards.

6.2 System Deployment

- Location: Call recording systems will be automatically implemented to monitor all calls received to the Contact Centre and Switch Board via our telephony provider.

Recordings will be saved securely in the telephony cloud system, for a maximum of 28 days upon which they will be automatically deleted. Where safety or security risks are identified the recording will be downloaded and stored securely within college systems.

- Usage: Authorised staff may use call recording systems for incident management and safeguarding concerns. Users must inform individuals they are being recorded.

6.3 Notification

The following notification shall be prominently announced at the start of calls: " Please note calls will be recorded for training, quality and security purposes. For more information as to your rights and the use of your personal data, please visit our website BMet.ac.uk and view our Call Recording Privacy Notice."

6.4 Data Management

- Retention Periods:
  - Automated recordings: Retained for 28 days.
  - Manually downloaded recordings: Retained longer if required for investigations. Recordings will be retained in compliance with the College Data Retention and Disposal Policy.
- Access Controls: Only authorised personnel will access or manage call recordings.

6.5 External Access Criteria

- Any recordings relating to a potential safeguarding concern may be shared with the appropriate external agency as relevant to the concern, with the approval of the Director of Student Experience and logged in MyConcern.
- Requests from police must include a completed WA170 form and will be processed by the Data Protection Officer.
- Data subject requests must include a completed Subject Access Request Form and evidence of identification and will be processed by the Data Protection Officer.
- All other third-party requests (e.g. contractors, insurers etc.) must be in writing (letter/email) with clear details as to the purpose of the request and justification for it. These requests will be processed by the Data Protection Officer.

7. Data Protection Impact Assessment (DPIA)

A DPIA will be conducted annually or when significant changes are made to the call recording system.

8. Training and Awareness

- Training will cover GDPR, DPA, Telecommunications Regulations and operational protocols.
- Training schedules (e.g., annual or biannual) will be determined and logged by the Contact Center Team Leader.

9. Monitoring and Review

Call recording systems will be reviewed annually for effectiveness and compliance.

10. Integration with Other Policies

This procedure aligns with the following:

- Safeguarding & Child Protection Policy
- Data Protection Policy
- Privacy Policy
- IT Security Policy