Data Use and Communications Policy

(UKMC Student Association - All Programmes)

Date	Author	Summary of Changes	Version	Authorised
24/06/2025	Dr Abbas Mohammed	New policy governing data use and communications by UKMCSA	1.0	Academic Board
Policy Owner	The policy is overseen by the Student Experience, Engagement and Employability Committee. Day-to-day implementation and communication responsibilities are delegated to the Student Engagement Lead, with oversight from the UKMC Data Protection Officer.			
Additional Responsible Parties	All UKMCSA Officers, Student Ambassadors, and Society Leaders who handle student data must comply with this policy and relevant data protection laws.			
Assessment	**Relevant Details**			
Equality Analysis	1. Completed in June 2025, aligned with UKMC, Equality, Diversity, and Inclusion Policy			
Legal	2. Aligned with the UK GDPR and Data Protection Act 2018			
Information Governance	3. Reviewed for compliance with UKMC data protection and confidentiality practices			
Student-Facing Procedures	4. Shaped by feedback from UKMCSA Officers and student representatives (May-June 2025)			
Consultation	**Relevant Contributions**			
Student Association via HR	Not Applicable			
Students via Course Reps (CRs)	Consultation via course evaluation and student engagement sessions (April 2025)			
Relevant External Stakeholders	Developed with reference to sector practice at UK higher education providers, and aligned with guidance issued by the Office for Students (OfS) and the Information Commissioner's Office (ICO).			
Other (if applicable)	Input from UKMC IT Services and Registry teams			
Authorisation and Version Control				
Authorised by	Academic Board			
Authorisation Date	24 June 2025			

Effective From	1 July 2025
Next Review Date	July 2027 (Biennial review, with reminder from Student Experience, Engagement and Employability Committee)
Document Access and Communication	
Document Location	UKMC Student-Facing Procedures page - [https://ukmc.ac.uk/policies-and-legislation]
Disseminatio n Plan	The policy will be distributed via UKMCSA training and induction sessions, officer and ambassador handbooks, official briefings and bulletins, Course Director meetings, and Student Portal notices

Contents

1. Introduction

The UKMC Student Association (UKMCSA) uses student data to support representation, events, and communications. This policy explains how that data must be handled responsibly and how official communications should be managed. It ensures that all activity complies with the UK GDPR, the Data Protection Act 2018, and UKMC's own policies.

2. Purpose

This policy ensures that all use of student data and communications by UKMC Student Association:

- Complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- Aligns with UKMC's IT and Data Security Policy 2024-25
- Respects the rights of students as data subjects.
- Provides clarity to all UKMCSA Officers and student leaders on what data they may access, how it must be used, and under what conditions.

3. Scope

This policy applies to:

- All UKMCSA Officers and Executive Committee members.
- All UKMC Ambassadors.
- All recognised Student Societies.
- Any other student leader or representative using student data on behalf of UKMCSA.

It covers data used for:

- Communication with students.
- Event promotion.
- Campaigns and elections.
- Representation and governance activities.

4. Legal Status and Data Governance

- Data Sharing Agreement: UKMCSA operates under a formal Data Sharing Agreement (DSA) with UKMC. No personal data from UKMC's Registry or

franchise partner universities shall be accessed, stored, or used without institutional authorisation and a recorded justification.

- Data Controller Role: UKMCSA acts as a data processor on behalf of UKMC and is bound by UKMC IT and Data Security Policy 2024-25, oversight, and governance structures.

5. Principles

5.1 UKMCSA will only process student data where there is a legal basis under GDPR:

- Legitimate interests for representative and association activities.
- Consent where required (e.g. mailing lists).
- Contractual obligations (e.g. prize winners for paid events).

5.2 Student data will be:

- Collected and processed fairly and lawfully.
- Used only for specified and legitimate purposes.
- Relevant and limited to what is necessary.
- Kept accurate and up to date.
- Stored securely.
- Retained according to the retention schedule below.
- Deleted securely once no longer needed.

6. Data Retention Schedule

Data Type	Retention Period	Deletion Method
Mailing lists	Officer term only	Secure deletion via UKMC platform
Event sign-up forms	6 months post-event	Encrypted deletion
Complaint-related data	In line with UKMC Student Conduct	Institutional deletion process
Images and videos	Until consent withdrawn or 3 years	Manual review and secure removal

Retention periods are justified on the basis of operational need, regulatory expectation, or legal risk, and will be reviewed periodically.

The Student Engagement Lead will supervise secure deletion and ensure destruction records are retained where required

6.1 What Data May Be Used?

Data Type	Purpose	Conditions for Use
Name and email address	Communications, event invitations, elections	Must be obtained from UKMC-authorised sources or with explicit consent
Course, year, campus	Inclusive communications and representation	Must be used solely for representation purposes
Student feedback	Inform representation and campaigns	Must be anonymised before external publication
Special category data	EDI work and targeted support	Explicit consent required; only where necessary
Photographs and video	Promotion, leadership visibility	Consent must be obtained for identifiable images

7. Data Sources and Access

- The UKMC Registry is the only authorised source of student data for UKMCSA purposes.
- Officers must request data via the Student Engagement Lead, with justification logged.
- Officers and Ambassadors must not collect or use contact details from:
    - Personal accounts.
    - Informal WhatsApp/social media groups.
    - Peer-shared spreadsheets or contact lists.

8. Communications with Students

8.1 UKMCSA communicates with students through:

- Official UKMC student email addresses (preferred).
- UKMCSA-managed and moderated social media platforms.
- Student Portal announcements.
- Posters and approved physical materials.

8.2 Safeguards for Mass Communication:

- All group emails must use UKMC-approved mailing tools.
- Officers must use BCC for group messages and never expose recipient lists.

- Each email must include an unsubscribe or opt-out option where appropriate.
- The Public Relations Officer must review and approve all bulk communications.

9. Consent, Privacy Notices, and Student Rights

9.1 UKMCSA will provide clear Privacy Notices for:

- Mailing lists.
- Event registration forms.
- Photography/video consent.
- Campaigns or surveys collecting personal data.

9.2 Managing Consent:

- Students may request minor internal correction or deletion of their personal data by contacting the Student Engagement Lead. However, any formal Subject Access Request (SAR) must be referred directly to the UKMC Data Protection Officer. UKMCSA cannot fulfil SARs and must not attempt to respond without referral
- Students may request access to any personal data held by UKMCSA in accordance with UKMC's Subject Access Request procedures.

10. Security and Storage

- Data must be stored only on UKMC-approved platforms (e.g. SharePoint, Microsoft Teams).
- Access is limited to authorised Officers and staff.
- Student personal or sensitive data must not be stored on personal devices. In very rare and exceptional circumstances, temporary local storage may be authorised under the UKMC IT and Data Security Policy, subject to encryption, secure transfer, and documented approval.
- Event/campaign data must be securely deleted when no longer required.

10.1. Cookie Use and Website Analytics

If UKMCSA operates websites or mailing platforms:

- UKMCSA platforms may use cookies for functionality and performance tracking.
- No personal data will be collected without user consent.
- Where analytics tools such as Google Analytics or Hotjar are used, users will be informed and given the option to opt out.

10.2. Photography and Media Use

- All photographs and videos must be captured using UKMC-approved devices or transferred promptly to secure storage.
- Consent is required for identifiable images used publicly.
- If a student withdraws consent, their image will be removed from websites and social media platforms within 5 working days.
- Media files must not be stored on personal devices unless approved.
- Tagging or sharing on social media must comply with consent terms.

11. Data Sharing and Disclosure

11.1 Student data may only be shared externally:

- With explicit student consent, or
- Where legally required.

11.2 UKMCSA will not:

- Sell or transfer data to third parties for marketing.
- Share mailing lists externally without a clear legal basis and consent.

All data sharing requests must be logged and approved by the Student Engagement Lead.

Any third-party platforms used for student data must comply with UKMC IT and Data Security Policy 2024-25 and UK GDPR, and must be approved before use.

12. Breaches and Reporting

12.1 Any suspected or actual breach must be reported immediately to:

- The Student Engagement Lead, and
- The UKMC Data Protection Officer.

12.2 Serious breaches may trigger:

- UKMC disciplinary action.
- Reporting to the Information Commissioner's Office (ICO).

13. Audit and Oversight

- The Student Engagement Lead is responsible for regular audits.

- Termly spot checks will be conducted on data access and use.
- Audit outcomes will be reported to the UKMC Data Protection Officer and relevant institutional committees.

14. Training and Support

All UKMCSA Officers, Ambassadors, and Society Leaders will receive:

- Basic training in UK GDPR and data protection.
- Ongoing guidance on responsible data use and privacy best practices.
- Training will be provided at induction and refreshed annually.

Refresher sessions will be mandatory if policy updates are made

Review and Approval

Approved by: Academic Board

Date of Approval: 28 June 2025