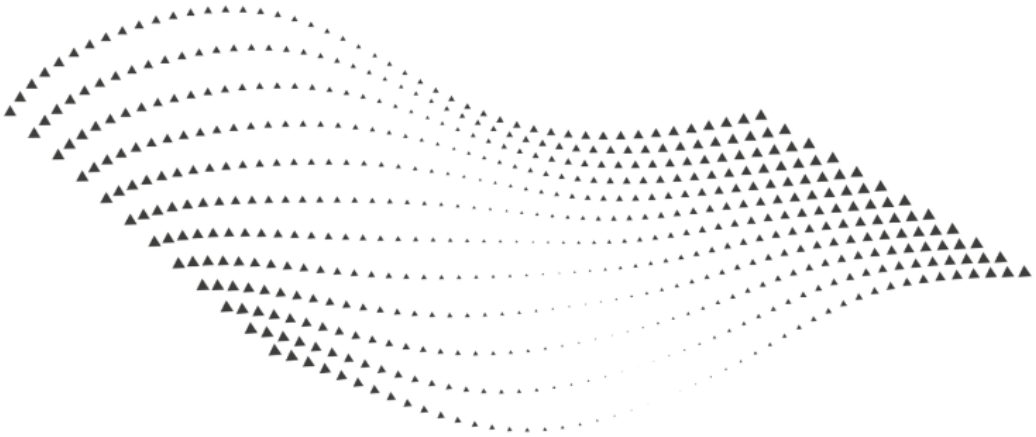
Data Protection Policy



Document Control					
Document No	POL001	Version	2	Version revision date	22/08/2025
Author	Benjamin Phillips	Approved by	Chief Financial Officer	Approved date	06/10/2025
Next review date	August 2027	Policy Owner	Head of Data	Department	Technology
Related policies, procedures, and records	Cyber and Information Security Policy Privacy Notice (BIMM Website) Cloud Data Storage Policy Record Retention Policy				

Data Protection Policy

Table of Contents

1. Introduction 3
2. Purpose 3
3. BIMM Structure 4
4. Data Protection Principles and Lawful Basis 4
5. Notification of Data Held and Processed 5
6. Information Governance Framework and Responsibilities 6
7. Data Subject Rights 8
8. Data Security 9
9. Data Breaches 9
10. Data Protection Impact Assessments 10
11. International Data Transfers 11
12. Supervisory Authorities 12
13. Publication of Information 13
14. Release of Personal Data to Official Bodies 13
15. Record Retention 13
16. Cookies and Similar Technologies 14
17. Personal Data for Marketing Purposes 14
18. Closed Circuit Television 14
19. Artificial Intelligence 15
20. Protection of Freedoms Act 2012 15

Data Protection Policy

1. Introduction

1.1. This policy deals with the appropriate acquisition, storage, processing, sharing and disposal of personal data by BIMM Group Limited, BIMM Universality Limited, Met Film School Limited and BIMM Dublin Limited. From here on in this document references to these organisations as a collective will be simplified to "BIMM".

1.2. In scope are all people (including permanent, fixed term, freelance, contracted, seconded, agency, volunteers, appreciates, interns, students), information, technologies, resources and facilities that deal with information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. Such identifiers are very wide and might include location data, or technology data, as well as the more obvious identifiers such as name.

1.3. Recognising the geographical reach of BIMM, references to data protection legislation include the following legislation:

- United Kingdom General Data Protection Regulation (UK GDPR);
- United Kingdom Data Protection Act 2018 (UK DPA2018);
- United Kingdom Data (Use and Access) Act 2018 (DUAA);
- European Union General Data Protection Regulation (EU GDPR);
- Irish Data Protection Act 2018 (Irish DPA2018);
- German Federal Data Protection Act / Bundesdatenschutzgesetz (BDSG);
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

1.4. BIMM has a duty to comply with the principles and requirements of data protection legislation. This policy is one way BIMM ensure data protection considerations are at the forefront of BIMM's activities including the processing of personal data. It also contributes towards an organisational culture of privacy by design and default.

2. Purpose

2.1. The purpose of this policy is to:

- Provide a framework for compliance with data protection legislation;
- Lay out the principles of the data protection legislation and define key terms in relation to BIMM;
- Make clear the scope and responsibilities of the BIMM community and to set out the governance structure for data protection issues;
- Outline the rights of data subjects;
- Provide overarching guidance on best practice and signpost to relevant policy, procedures, and committee activities.

3. BIMM Structure

3.1. BIMM is formed of four separate legal entities. There is a business requirement for personal data to be shared between the entities to provide a complete, consolidated, streamlined and global services to students and to effectively manage staff wherever they may be in the world.

3.2. BIMM have established an intra group data sharing agreement. This document governs when and how data may be shared within BIMM and the circumstances where data cannot be shared to meet confidentiality, regulatory and statutory requirements. It also establishes responsibilities for compliance with data protection legislation such as how BIMM manage data subject requests and the reporting of personal data breaches. The document defines safeguards to protect that data, both inside BIMM and with third parties.

3.3. Queries on the content and application of the intra group data sharing agreement should be directed to the Head of Data or the Chief Financial Officer.

4. Data Protection Principles and Lawful Basis

4.1. The term “processing” in this context is the same as defined in Article 4(2) of the UK GDPR. That definition being any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.2. The UK GDPR and EU GDPR outline the key principles which protect the fundamental rights and freedoms of data subjects. All personal data processed by BIMM shall be:

- Obtained and processed lawfully, fairly and transparently.
- Obtained for specified and legitimate purposes and shall not be further processed in any manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Not be transferred to another party, such as a company that processes our data on our behalf, or a business partner, unless they can provide evidence that they are compliant with the data protection principles and have successfully completed the procurement process. All contracts with such parties shall include the standard terms that include compliance with data protection legislation or refer to an established data sharing agreement.

4.3. BIMM must have a lawful basis for processing personal data. The lawful basis are:

- Contract: Processing is necessary for the performance of a contract to which the individual (data subject) is party or in order to take steps at the request of the individual prior to entering into a contract.
- Legal Obligation: Processing is necessary for compliance with common law or statutory obligations.
- Vital Interests: Processing is necessary to protect someone's life.
- Public Task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- Legitimate Interests: Where personal data is used in ways individuals would reasonably expect it to be used and which have minimal privacy impact.
- Recognised Legitimate Interests: When BIMM use personal information for certain 'recognised legitimate interests', it removes the need to balance the impact on the people whose personal information are used, against the benefits arising from that use. This lawful basis was introduced under the DUAA.
- Consent: The individual (data subject) has given their consent based on a very clear and specific statement of consent. There are other rules around consent such as requiring positive opt-in and simplifying withdrawal of consent. Consent must only be used where BIMM cannot rely upon an alternative lawful basis. Consent can be easily withdrawn with minimal notice at which point all processing of the data must stop.

4.4. Processing of sensitive personal data, for example information about a person's health, criminal convictions or protected characteristics, require an Article 9 condition. When relying upon consent, BIMM will collect explicit consent prior to the collection and processing of sensitive personal data.

5. Notification of Data Held and Processed

5.1. One of the rights under UK GDPR and EU GDPR is the right to be informed. This right is fulfilled through the use of privacy notices and information provided at the time of data collection.

5.2. All staff, students, clients and anyone about whom BIMM processes personal data shall:

- Know what information BIMM holds and processes about them and why;
- Know how to gain access to the stored data;
- Be aware of the procedures in place to keep the data up to date;

- Know what BIMM is doing to comply with its obligations under data protection legislation and associated regulations;
- Know how to contact the Data Protection Officer;
- Know how to lodge any complaint with BIMM; and
- Know how to lodge any complaint with the Information Commissioner's Office.

5.3. Where there is a change in the way BIMM process personal data, this will be communicated through an update to the privacy notice and made accessible to all data subjects.

5.4. The People Team shall, at set intervals, ask every member of staff to review their personal data stored on the Human Resources database using the self-service function.

6. Information Governance Framework and Responsibilities

6.1. BIMM operate an information governance framework, providing a structured approach to data protection compliance and providing clear responsibilities and accountabilities for this compliance. This ensures BIMM adopt best practice governance and comply with data protection legislation.

6.2. All staff

6.2.1 Staff are responsible for familiarising themselves with this policy and to be aware of their roles and duties in relation to data protection.

6.2.2 Staff are responsible for ensuring that they complete all data protection training as required by BIMM at least once every two years.

6.2.3 Staff are responsible for ensuring they report any personal data breaches they become aware of immediately by emailing privacy@bimm.co.uk with all information concerning the breach.

6.2.4 Any staff commencing a new project must consider data protection at all stages of the project's lifecycle and manage the privacy risk to a level that is agreed as acceptable (see Data Protection Impact Assessments).

6.3. Data Protection Officer

6.3.1 BIMM are required to appoint a Data Protection Officer. The Data Protection Officer is the Head of Data and represents all entities of the Group. They oversee the work of the privacy function including monitoring compliance with data protection and freedom of information legislation, facilitate data subject access requests and personal data breaches.

6.3.2 Article 39 of the GDPR outlines their statutory tasks:

- To inform and advise BIMM employees, including the senior management team, and any third parties who carry out processing, of their obligations pursuant to data protection legislation;
- To monitor compliance with data protection legislation, with BIMM policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested on data protection impact assessments and monitor their performance;
- To cooperate with supervisory authorities;
- To act as the point of contact for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR and to consult, where appropriate, with regard to any other matter.

6.4. Executive Management Group

6.4.1 The Chief Financial Officer is the relevant member of the Executive Management Group who has overall responsibility for data protection and information governance.

6.5. All members of the Executive Management Group will:

6.5.1 Promote a proactive, positive culture of data protection compliance and of privacy by design and default;

6.5.2 Demonstrate accountability for data protection through leadership, support, and allocation of necessary resources;

6.5.3 To remain informed of changes to data protection laws and their impact upon BIMM;

6.5.4 To support risk management processes relating to personal data processing activities.

6.6. Data Governance SteerCo

6.6.1 The Data Governance SteerCo provides direction and guidance across BIMM on data protection and information governance activities. This is achieved by:

- Supporting and driving data protection and information governance action plans;
- Providing a critical review of key performance indicators, data and IT security risks and casework;
- Overseeing the participation in external and internal audits and the completion of audit action plans;

- Contributing to discussions of issues relating to data security, privacy, and I.T infrastructure to ensure that these align with BIMM's strategic plans.

6.7. Data Asset Owners

6.7.1 BIMM have identified data asset owners who act as custodians for personal and business datasets processed by and on behalf of BIMM.

6.7.2 Data asset owners are listed in the data retention policy.

6.8. Data asset owners will:

6.8.1 Ensure that personal data within their remit is processed lawfully, fairly, and transparently;

6.8.2 Support the Data Protection Officer in the creation and revision of a record of processing activity and other compliance documentation;

6.8.3 Support the Data Protection Officer in the facilitation of data subject right requests;

6.8.4 Periodically review the necessity, accuracy, and retention of personal data within their remit.

7. Data Subject Rights

7.1. Data protection legislation gives individuals, known as data subjects, rights. All individuals have the following rights:

- To be informed about the collection and use of their personal data.
- To access their personal data and supplementary information.
- To have inaccurate personal data rectified or completed if it is incomplete.
- To have personal data erased.
- To request the restriction or suppression of their personal data.
- To data portability, enabling them to obtain and reuse their personal data for their own purposes across different services.
- To object to processing based on 'legitimate interests'; for the purposes of direct marketing and for certain types of research.
- To challenge automated decision-making and profiling
- To raise any complaint about the way BIMM process personal data.

7.2. Any of the above data requests can be received by any staff member. If received, they should be forwarded on to privacy@bimm.ac.uk without delay. All data

requests will be facilitated by the privacy team with support of colleagues across BIMM.

7.3. Any complaint about the way BIMM process personal data should be raised in line with the complaints policy. Complaints should be made for the attention of the Data Protection Officer via the standard complaint process.

7.4. Persons on whom BIMM holds data have the right to access any of the personal data that is processed about them. The request, known as a Subject Access Request (DSAR), should be made to the privacy team (privacy@bimm.ac.uk) and accompanied by a proof of identity (see Annex A). In most cases the DSAR can be made free of charge. If a charge is applicable, then individuals will be contacted to arrange payment. The DSAR must include enough information to enable BIMM to conduct a reasonable search to find the personal data being requested, without excessive effort.

8. Data Security

8.1. Staff have a responsibility to protect personal data assets. This responsibility applies to all records regardless of whether they are stored in a digital or physical format.

8.2. Consideration should be given to the sensitivity of physical records with due consideration for both security protections (e.g. against theft) and environmental protections (e.g. against fire and flood).

8.3. Records stored on a computer system must be held securely with access only available to those who require it. Holding personal data on removable media or mobile devices is discouraged and the use of encryption is mandatory in these cases.

8.4. Data must only be stored or transferred using approved BIMM systems. The introduction of new IT systems and cloud storage providers must follow the procurement process and a data privacy impact assessment must be completed and approved before any data is uploaded to the system.

8.5. Official communications must only take place through approved BIMM communication methods. Communication through personal messaging services including text message, WhatsApp and non-BIMM email accounts is prohibited.

9. Data Breaches

9.1. All staff are expected to be vigilant to the possibility of breaches of this policy or to the principles of data protection legislation.

9.2. A personal data breach in this context is the same as defined in Article 4(12) of the UK GDPR. That definition being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

9.3. All data breaches and suspected data breaches must be reported to the privacy team (privacy@bimm.ac.uk) without undue delay. There are strict timescales for reporting any such breach to affected individuals and the relevant authorities.

9.4. The privacy team will internally log all data breaches and near misses. This will include an assessment of risk and advice on any mitigating actions which must be taken to contain a breach.

9.5. All breaches, unless unlikely to result in a risk to the rights and freedoms of natural persons, shall be reported to a supervisory authority. Where feasible the report will be made within 72 hours. The privacy team will make this notification on behalf of the BIMM entity who is the data controller in the context of the breach. Depending on the scope of the breach, this may be reportable to the Information Commissioner's Office, Data Protection Commission (Ireland) or both supervisory authorities.

9.6. All breaches, unless unlikely to result in a high risk to the rights and freedoms of natural persons, shall be reported to the data subject. The privacy team will advise on the content and method of communication.

10.Data Protection Impact Assessments

10.1. A data protection impact assessment is in essence a risk assessment of privacy considerations for a form of data processing. Both UK GDPR and EU GDPR mandate the completion of a data protection impact assessment where a type of processing is likely to result in a high risk to the rights and freedoms of an individual. This could apply to a change of a process / procedure or the introduction of new technologies.

10.2. A data privacy impact assessment should not be viewed as a barrier to new projects but a mechanism of ensuring data security and privacy considerations have been considered early within the project and people's data remain secure.

10.3. BIMM have a template document for the completion of a data protection impact assessment. The template includes a set of screening questions to identify the level of risk. Completed assessments should be kept by the privacy team and saved alongside the system / project files.

10.4. You are required to consult the Data Protection Officer in the completion of a data privacy impact assessment (privacy@bimm.ac.uk).

11.International Data Transfers

11.1. The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, regardless of the size of transfer or how often data is transferred. EU GDPR applies similar restrictions.

11.2. Restricted transfers must only be made where there is an adequacy agreement approved by the Secretary of State or where the transfer is covered by appropriate safeguards.

11.3. UK adequacy is granted by a Secretary of State. As well as designating a country to be adequate, the Secretary of State can also designate territories within a country, sectors of an economy, and international organisations as adequate.

11.4. In exceptional circumstances, a transfer can take place when covered under one of the UK GDPR Article 49 exemptions. An exemption must not be used without prior consultation with the Data Protection Officer.

11.5. It should be noted following the Brexit transition period, the UK government determines which countries and territories are awarded adequacy status and these may differ from an adequacy status granted by the European Commission under EU GDPR.

11.6. As of July 2025 the following countries / territories have been granted an adequacy decision by the UK government:

Andorra	Germany	Luxembourg
Argentina	Gibraltar	Malta
Austria	Greece	Netherlands
Belgium	Guernsey	New Zealand
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Isle of Man	Romania
Denmark	Israel	Slovakia
Estonia	Italy	Slovenia
Faroe Islands	Jersey	Spain
Finland	Latvia	Sweden
France	Liechtenstein	Switzerland

The Republic of Korea Lithuania Uruguay

Canada - only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
Japan - only covers personal data transferred to private sector organisations falling within the scope of Japan's Act on the Protection of Personal Information (APPI) by Personal Information Handling Business Operators (PIHBOs) within the meaning of the APPI.
The United States of America - only covers data which is transferred under the UK Extension to the EU-US Data Privacy Framework.

12.Supervisory Authorities

12.1. BIMM operate within the UK and Europe. The UK and each member state of the European Union have provided an independent public authority, known as a supervisory authority, who are responsible for monitoring the application of data protection laws, protecting the fundamental rights and freedoms of individuals and in the case of Europe facility the free flow of personal data within the Union.

12.2. The supervisory authority for the United Kingdom is the Information Commissioner's Office. BIMM's UK entities are registered as data controllers with the Information Commissioner's Office and appear within the register of fee payers. These registrations are:

- **Name:** BIMM Group Limited
- **ICO Registration Number:** ZB726298

- **Name:** BIMM University Limited
- **ICO Registration Number:** ZA362716

- **Name:** Met Film School Limited
- **ICO Registration Number**: Z228019X

12.3. Where BIMM operate within the European Union or process the personal data of those within the union, there is a requirement to cooperate with European supervisory authorities.

12.4. BIMM have nominated the Data Protection Commission (Ireland) as their competent EU supervisory authority under the one stop shop mechanism. This means the Data Protection Commission (Ireland) will act as the lead supervisory authority for any personal data breach or complaint under the EU GDPR.

12.5. The Head of Data, in their capacity as BIMM's Data Protection Officer, is the main point of contact for all communication with the supervisory authorities.

13. Publication of Information

13.1. The following will be available to the public for inspection:
- Names and job titles of BIMM staff.
- Summary details of student achievement and examination successes.
- Details relating to an individual student, including participation in productions and events related to or resulting from their studies, will not be published without the express permission of that individual.

13.2. BIMM University is subject to the Freedom of Information Act 2000. Personal information about identifiable persons will not be made public unless permittable under the Act.

14. Release of Personal Data to Official Bodies

14.1. BIMM have certain obligations which requires it to share data with official (statutory) bodies, the Students Union and other such organisations.

14.2. BIMM also have statutory obligations to, on request, provide the police and national security officers with staff/student data, including CCTV images.

14.3. Except in an emergency, all such requests will be referred to the privacy team and assessed against the relevant sections of data protection legislation.

14.4. All requests for personal data by official bodies must be made in writing.

14.5. Requests from UK law enforcement agencies will be asked to provide a signed 'request to external organisation for disclosure of personal data to the police form' also known as a 'DP2' alongside their request. Requests from international law enforcement agencies should be accompanied by the equivalent paperwork.

15. Record Retention

15.1. BIMM maintain a separate record retention policy which can be accessed from BIMMNet.

15.2. The policy outlines how long BIMM will retain records for, and appropriate methods of record disposal based on statutory, contractual and business requirements.

15.3. This policy is designed to support the principle of data minimisation.

16.Cookies and Similar Technologies

16.1. Cookies are pieces of data that are downloaded to a web browser by a website and allow the device to be recognised by the website on subsequent visits. They are often used for tracking of visitor activity and to provide a cohesive user experiences for returning visitors.

16.2. Legislation requires that consent is sought for the use of cookies for some purposes. Any use of cookies or similar technologies on BIMM websites must be assessed against the legislation to decide whether consent from visitors is required for the use of this technology.

16.3. BIMM websites will contain cookie banners and dedicated cookie notices where required.

17.Personal Data for Marketing Purposes

17.1. In accordance with Data Protection legislation, BIMM will obtain consent from individuals for the collection and processing of data for direct marketing purposes.

17.2. Marketing consent will be 'opt-in'.

17.3. All new proposals for processing personal data for marketing purposes shall be vetted by the Director of Marketing or a person designed by them.

17.4. Where marketing activities rely upon the lawful basis of legitimate interests, BIMM will document a legitimate interest assessment and inform the individual during the first communication of how their details were obtained and why they have received the marketing material.

17.5. All marketing communications will include the option to unsubscribe from future marketing material.

18.Closed Circuit Television

18.1. BIMM operate CCTV systems for the purposes of security and safety. Where such systems are in use, appropriate signage will be displayed on the site.

18.2. Subject access requests for CCTV data will be dealt with in the same way as access to any other form of personal data.

18.3. CCTV images may contain other individuals who are recognisable. Individuals who are recognisable must provide their consent before their image can be shared. If the individual does not consent or if consent cannot be obtained, their image must be pixelated or blurred before footage shall be provided.

18.4. The DPA2018 gives BIMM the right to refuse a request for a copy of the CCTV image, particularly where access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders or affect the privacy of another individual.

19.Artificial Intelligence

19.1. The use of any artificial intelligence that involves personal data must be subject to the data protection impact assessment process.

19.2. Article 22 of the UK GDPR and EU GDPR outline a data subject's right in relation to automated decision making and profiling. Where BIMM make decisions about an individual solely based on automated processing, BIMM must be able to provide human intervention to consider alternative points of view and any contest of the automated decision.

20.Protection of Freedoms Act 2012

20.1. The Protection of Freedoms Act 2012 details the legal obligations relating to the storage, use and destruction of biometric data (for example, fingerprints and DNA). BIMM does not store and use biometric data.

Annex A

When processing a data rights request BIMM must be satisfied that they know the identity of the requester (or the person the request is made on behalf of); and the data held relates to the individual in question (eg when an individual has similar identifying details to another person). For this reason requestors may be asked to provide a copy of official government-issued identification before their request is accepted.

The following forms of photographic identity are accepted by BIMM:

- Driving licence
- Passport
- Forces identity card

If the requestor asks for documents to be provided in a printed format, proof of address may also be requested to ensure the security of documents in transport. The following documents are accepted by BIMM:

- Bank statement dated in the last three months
- Utility bill dated in the last three months