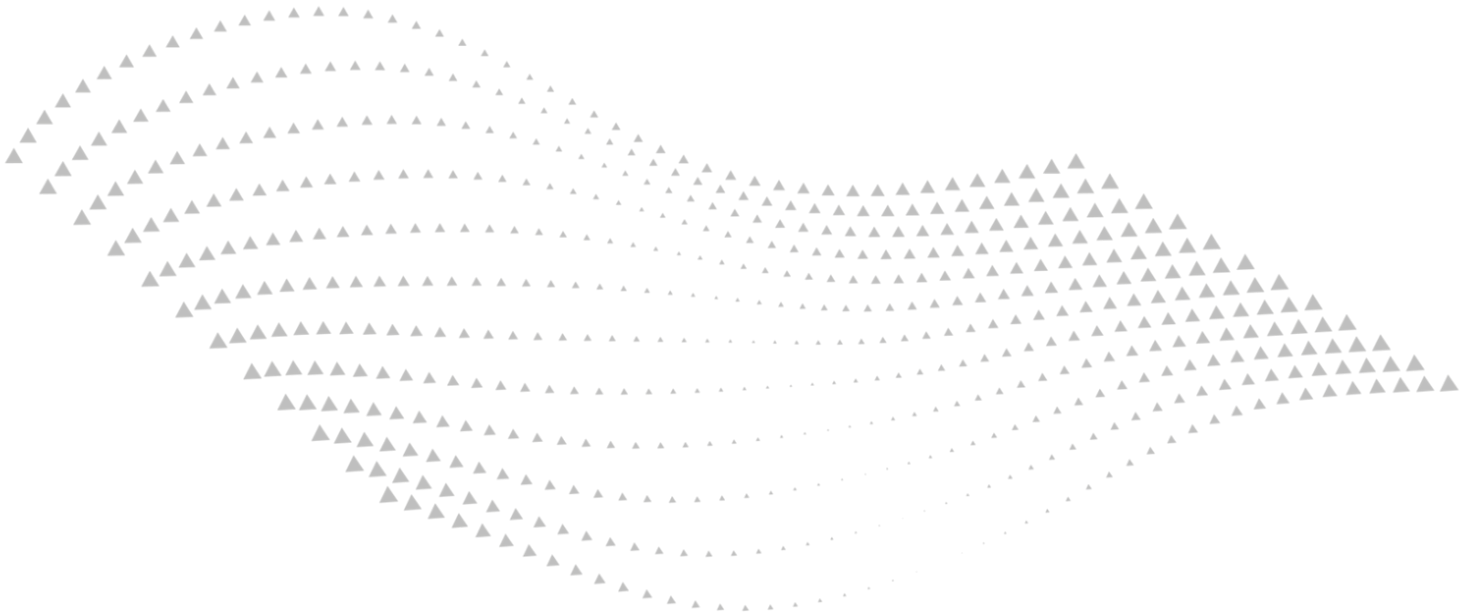
BIMM UNIVERSITY | A university for the creative industries

Research Data Governance Policy



Last approved: May 2022

Approved by: Academic Board

Next review due: May 2026

Introduction

This Policy applies to all students registered on a course at BIMM University and to all staff employed by the University, irrespective of their contract type.

Where research conducted under the auspices of the University is governed by a professional body, or funded externally, it is important to note that where there is any discrepancy, the data management regulations and policies put in place by research funders or other professional bodies shall take precedence over this policy.

This Policy should be read and considered alongside:
- The University's Ethical Review Policy & Procedure
- For students, the Student Intellectual Property Policy, as research data and other findings of research constitute the researcher's Intellectual Property.
- For staff, the information they are provided by the University regarding Intellectual Property and the Staff Data Protection Policy.

Value of Research Data Governance Policies

From a legal perspective:
1) To ensure all stakeholders recognise their responsibilities and obligations in relation to research data and data subjects. This includes their legal obligations and responsibilities, particularly in relation to **General Data Protection Regulation** and the Data Protection Act 2018.
2) To minimise the risk of reputational damage and/or litigation from lost, stolen, or intercepted data.

From an academic perspective:
1) To contribute to data being maintained and preserved as identifiable, discoverable, retrievable and reusable assets which are accurate, complete, authentic and reliable. This assists with the ambition to foster the open exchange of ideas, keeping research open to scrutiny and debate.
2) To contribute to maintaining the highest standards in research.

From an ethical perspective:
1) To ensure the privacy, dignity, rights, safety and wellbeing of all involved in research, and avoiding unreasonable risk or harm to research participants, researchers and others.

Legal Frameworks

Researchers must ensure compliance with all relevant legal, ethical and regulatory frameworks in the nation or nations within which they are working. The University operates in three territories – the UK, the Republic of Ireland and Germany.

In all three territories, researchers must comply with the General Data Protection Regulation (GDPR) 2018[1], which governs the collection, use and storage of personal data (that is, information which, directly or indirectly, could identify a living person, including online identifiers and IP addresses). The GDPR also stipulates particular considerations in relation to 'sensitive data' (or 'special categories of personal data'), which includes race and ethnicity; political stances; religious beliefs; trade union membership; physical and mental health conditions; sexual orientation; criminal files and court proceedings; biometric data; and genetic data.

Researchers should also be aware of the Freedom of Information Act (2000).

[1] Following the UK's exit from the EU, both EU countries and the UK are broadly following the same principles originally laid out in the EU GDPR.

Defining Research Data

Research data refers to all data used, collected or generated during the course of a research project. The term 'research data' encompasses data in many different formats. This includes, but is not limited to: Text (PDF, doc, rtf, txt); Images (RAW, JPEG, PNG); Databases (Excel, Access); Multi-media, video and audio (QuickTime; mp3, mp4); Software; 3D and statistical models; Hard copies (logs, field notebooks, diaries, workshop notes, sketches, questionnaires); Correspondence (email, handwritten letters); Inputs and outputs of simulations and models.

While the majority of this policy document concerns data collected or generated during the course of a research project, it is also important to consider the use of existing datasets. Please see below for further information in this regard.

Broadly speaking, research data falls into two categories:

1) **Personally Identifiable Data** (Information sheets; consent forms, completed questionnaires, audio tapes, transcripts, etc)
2) **Anonymised Data.**

These two different types of data require different management. As far as possible, all research data should be anonymised.

Anonymisation protects the identity of participants and allows research data to be shared with third parties, while preserving confidentiality. Personally identifiable information should never be disclosed from research data, unless a participant has given their consent to do so, in writing. The goal of the researcher applying anonymisation is to render data unattributable to an individual or group, while preserving the connected elements in the data that are relevant to the research being undertaken.

Typically, participants can be identified in research data through two means:

1) **Direct identifiers** such as name, address, video, pictures, or other information.
2) **Indirect identifiers** when combined with other available data could lead to the identification of a participant, such as workplace, occupation, salary or age.

Data is anonymised by permanently removing all direct identifiers and replacing them with codes, while indirect identifiers are either generalised or aggregated so that they are no longer attributable to a single participant or subgroup. This approach is commonly used when working with quantitative data.
Pseudonymisation is an alternative method of managing personally identifiable data by using artificial identifiers like an alternative name, and disguising identifiable information such as locations, organisations, and dates. Typically, this approach is used when working with qualitative data where context and situational information from participants may be of particular importance to the research focus, and anonymisation in its full application would not adequately preserve dependant variables or the contextual element in the data that is within the scope of the research.

With each approach there is a degree to which the chosen method can be applied more, or less, to achieve the required balance of participant confidentiality while maintaining the information contained in the data that is of value to the research. For example, when considering what specific information should be redacted from an interview transcript with a participant, researchers need to be clear about what information is within the scope of the project, and what information is not, and furthermore what must be changed or removed to protect the identity of the participant.

The right approach will depend largely on the nature of the research being undertaken and the research methodology being employed. It should be noted that removing key variables and contextual information from data could result in missed details or incorrect inferences during analysis. Therefore, it is advised that the appropriate method and degree to which it will be applied is carefully considered in the project planning stage, so that it may be confirmed with participants during the informed consent

process, prior to the commencement of data capture. This is especially helpful when conducting research involving interviews with participants, where the parameters of what is relevant to the research and what is not can be agreed with participants beforehand, so that transcripts do not require significant redaction to protect identities.

Anonymisation is generally the preferred approach to managing research data, except where to do so would prevent the use of the data by third parties in the future if the data is stored at the end of the project lifecycle. In this case, careful pseudonymisation should be used.

For detailed guidance on the application of anonymity and pseudonymisation to research data, including examples, please visit Research data management — UK Data Service.

Scope & Responsibilities

This policy covers all research activities conducted within, or under the auspices of the University, with particular significance for those research projects which generate data and/or may result in publications or other similar outputs. It therefore applies to all employees engaged in research, students of the University, and others undertaking research using University facilities or premises.

Supervisors have a responsibility to ensure their students are suitably informed regarding research ethics, effective data management, and their legal obligations.

The University is committed to supporting researchers in their obligations to comply with this policy. It commends the free online training course offered by Research Data MANTRA which offers guidance for all who work with digital data as part of their research. The modules 'Data Management Planning,' 'Storage and Security,' and 'Protecting Sensitive Data' are particularly applicable to research at the University and should take approximately one hour each to complete.

The University also commits to reviewing this policy and its effective implementation on a regular basis. It will ensure that there are appropriately qualified and experienced members of staff available to respond to queries related to the contents and implementation of this policy.

Queries or concerns related to this policy should be directed, in the first instance, to the chair of the University's Research & Enterprise Committee.

Data Management Plan

Before any data collection or generation begins, a Data Management Plan must be completed as part of the ethical approval process. This must cover:

- The types of data which will be collected
- Methods of data collection
- Methods of data analysis
- Methods for suitable anonymisation and/or pseudonymization
- Provisions in place for secure short-term storage
- Expectations for how data will be used
- Data sharing and access during the project lifecycle
- Expectations for long-term preservation
- Retention period
- Plans for secure disposal

We encourage you to use the template available here on our website.

For collaborative research projects, the primary responsibility for the creation, implementation and maintenance of the DMP lies primarily with the PI or Lead Researcher, as appropriate (though all researchers hold responsibility for its implementation). For students at the University, this responsibility lies dually with students and those supervising their research projects.

The DMP should be kept updated throughout the research project's lifecycle, and any significant changes should be highlighted to the Ethical Approval Committee, so that any new ethical concerns can be addressed.

Data Management Recommendations & Expectations

Gathering Data

Except where it is impossible in relation to the project aims, all data gathered during the course of research should be governed by the principle of informed consent. This means that research participants are informed, whether in writing or verbally, of how their data is going to be stored, used and disseminated.[2] Where interviews are to be recorded, written consent should be obtained. Researchers must be transparent about the data processing that they are going to undertake. Participants must be told who has access to personal information relating to the study, including any necessary wider disclosures (including, but not limited to, supervisors, transcribers and translators).

In line with GDPR, personal data can only be collected and stored for the specific purposes declared at the time of collection. It cannot be used for purposes other than these, nor passed on to others for different purposes. The data collected should be relevant and sufficient for the project's purposes, and not excessive.

Secure Storage

Researchers have a responsibility to ensure that research data is maximally secured. Where research cannot be suitably anonymised or pseudonymised, this means giving particular consideration to ensuring that data is not disclosed to unauthorised recipients.

Storing Personal Identifiable Data

There must be adequate safeguards in place to protect personal data while it is being stored for research purposes. Researchers should have a specific primary location in which this data will be stored, and a specific secondary location in which it will be backed up. As far as possible, Personally Identifiable Data should not be stored in any further locations. It is very important that any keys or records which would allow the linking of anonymised data with Personally Identifiable Data are not stored together.

We strongly encourage staff and students to use the OneDrive facility linked to their University account, as this complies to the required security standards. Researchers may either use this as the primary or the secondary data location.

All Personally Identifiable Data stored on portable electronic devices (including mobile phones, tablets, laptops, and external hard drives) must be encrypted. External devices such as USBs are strongly advised against as these can be easily lost or damaged and thus provide minimal security. The University's IT services can provide expert advice on encryption (please contact your local IT support team). It is also strongly advised that such portable electronic devices are securely stored, ideally in a locked cabinet.

[2] In line with UKRI guidance, it is sufficient to request 'broad consent to maximise data-sharing' and thus researchers are not expected to have a fixed list of proposed publications and outputs at the outset of the project. However, as the project progresses, it may be appropriate to update your data management plan with details of any outputs, and to consult with the Ethical Approval Committee regarding any data sharing concerns this may incur.

If other temporary storage facilities are to be used (cloud; hard copies) then every effort should be made to ensure that these are secure. Hard copies should be stored in a locked cabinet. This is also the case if hard copies of consent forms are to be retained.

It is strongly recommended that Personally Identifiable Data gathered during the course of a research project is not transferred using email, for it cannot be guaranteed that this will transfer documents securely.

Periodic checks should be used to ensure that the data are safe.

Personally Identifiable Data must not be kept for any longer than necessary for the purposes of the research project.

Storing Data

As noted above, all research data should be anonymised or pseudonymised as far as possible. This applies to its short-term storage, long-term storage, and dissemination.

As with Personally Identifiable Data, it is strongly recommended that researchers have a primary location in which anonymised and or pseudonymised data is stored, and a specific secondary location in which it will be backed up. As far as possible, anonymised and pseudonymised data should not be stored in any further locations.

We strongly encourage staff and students to use the OneDrive facility linked to their University account, as this complies to the required security standards. Researchers may either use this as the primary or the secondary data location.

All anonymised data stored on portable electronic devices (including mobile phones, tablets, laptops, external hard drives and USBs) should be encrypted. The University's IT services can provide expert advice on encryption (please contact your local IT support team). It is also strongly advised that such portable electronic devices are securely stored, ideally in a locked cabinet, as well as password protected.

Wherever possible, anonymised data should not be stored in hard copy format. Where this is unavoidable, the DMP must detail which measures are being taken to ensure the security of the data (for example, storage in a personal locker.)

Where temporary storage measures (e.g., Cloud, USB, personal laptop) are used, this should be kept to a minimum, and all data transferred back to the university network as soon as practicable, with any temporary copies of data securely destroyed. Periodic checks should be used to ensure that the data Is safe.

Some professional bodies and funding bodies also operate their own networks and data storage areas. Please check their policies to determine whether they prefer that researchers operating under their auspices prefer them to use these, whether exclusively or in addition to those provided by the University. Any anonymised and pseudonymised data transferred via the internet (for example, via email) should be encrypted.

Researchers have a responsibility to ensure that their data is rationalised and organised. Researchers should also keep clear and accurate records of their research methods and processes. This is a matter of both proper research conduct, but also of being prepared for potential questions about research conduct and results.

Preservation

Preserving Personal Identifiable Data

In keeping with GDPR data retention periods for Personally Identifiable Data should be kept to an absolute minimum, and with due consideration for its security, as above. As a guideline:

- UG/PGT – retained for one full academic year after the award of the degree (unless an external ethics panel suggests otherwise);
- Staff – 5 years after the final completion of the research (usually the data of publication, or presentation to sponsor), unless part of a longitudinal study, or another ethical body requires otherwise. Where there is no publication, 5 years from the completion of fieldwork.

Preserving Data

Once data has been anonymised or pseudonymised and there is no link through personal data, including birth date and record numbers, to an individual, and all codes to enable any linking have been destroyed to the best of your ability, research data can be held indefinitely on secure computers and servers.
Researchers must also consider the value of making their research data openly accessible after the end of the project's lifecycle. This is normal practice where:

- The research data has acknowledged or expected long-term value;
- The research data supports published research outputs;
- The research has been funded by a Research Council, or other public money. As stated in UKRI guidance, 'publicly funded research data are a public good, produced in the public interest [and] should be openly available to the maximum extent possible.'

This may mean retaining a whole dataset or determining which parts of a dataset ought to be preserved.

For staff projects, determining which, if any, parts of a research dataset ought to be preserved is the responsibility of the PI or lead researcher(s). For student projects, it is highly recommended that students work with their supervisors to consider whether/which data should be preserved. Due consideration should be given to the format in which data will be preserved, to ensure it can be accessed at a future date. The University recommends consulting this guide, produced by the Digital Curation Centre, for guidance on deciding which data ought to be retained.

Length of Retention

In line with UK research council guidance, it is expected that anonymised data relating to research projects will be stored securely for ten years upon the completion of a research project, in both paper and digital formats. Where there is any discrepancy, data retention periods specified by research councils, and other professional and funding bodies, supersede the provisions in this policy.

Datasets may be retained for longer than the normal 10 years where:

- A statutory obligation/contractual obligation/funding body requires it
- The research results have resulted in a patent application
- The results have become contentious or subject to challenge during the previously agreed retention period
- The research has a public interest or longer-term value.

Data Repositories

The University supports the principles of Open Access, echoing the UKRI guidance on best practice in the management of research data, which states, 'widespread sharing of data will enable researchers, empower citizens and convey academic, economic and social benefits.'

As such, we encourage researchers to consider making anonymised research data accessible to third parties via a data repository, subject to limitations imposed by legislation and general principles of confidentiality. We also encourage researchers – particularly staff – to explore the affordances of ORCiD, a free service providing unique, persistent identifiers for individuals to use as they engage in research. More information can be found on ORCiD's website.

Disposal

Disposing of Personal Identifiable Data

When no longer required, all personal identifiable data pertaining to a project must be securely destroyed. This is the responsibility of the researcher, up to and including the point of destruction.
IT Services can provide advice on securely destroying data stored electronically (please contact your local IT support team).

Disposing of Anonymised or Pseudonymised Data

Where anonymised or pseudonymised data Is to be destroyed, either because the period of retention has ended, or because it is not deemed worthy of preservation, this must also take place in a legal, ethical, and regulatorily consistent manner, and with particular concern for confidentiality and security. The University securely disposes of hard copies of data through a certified shredding company, which students can make use of If they consult the reception staff in their local college or in the case of students the college Estates Team. Where appropriate, consult your funder or organisation's requirements for the disposal of data.

Third Parties and Other Stakeholders

In some circumstances, research may be conducted in partnership or under contract with a third party. In these circumstances, a data sharing, or collaboration agreement should be signed before the start of the research. This should include a clear policy regarding data ownership and partner responsibility for data governance, management and storage.

Disciplinary Procedures

The University will investigate all allegations that any person conducting research on behalf of or within the University has not adhered to the guidelines within this Policy. For students, this will be in accordance with the misconduct procedures set out in the Academic Regulations. For staff, this will be in accordance with the disciplinary procedures set out in their employment contracts.

If you have concerns about the conduct of a researcher operating under the auspices of the University, please report these to the chair of the Research & Enterprise Committee.

Use of Existing Datasets

All users of research data generated by others must acknowledge the data sources and abide by any attendant Terms and Conditions.

Steps should be taken to ensure that any data generated by others and used for research purposes under the auspices of the University are securely stored, and any copies appropriately destroyed upon completion of the research project, using the same principles as detailed above for anonymised data.

Further Information & Training

For further information, the University commends the below resources. While these are produced by other UK Higher Education Institutions, they contain a great deal of information which is transferrable across institutions. Since they both use GDPR as their primary legal framework, they are also relevant across the UK, the Republic of Ireland, and Germany.

Research Data MANTRA is a free online course which offers guidance for all who work with digital data as part of their research. The modules 'Data Management Planning,' 'Storage and Security,' and 'Protecting Sensitive Data' are particularly applicable to research at the University and should take approximately one hour each to complete.

The Research Data Management webpages hosted by the University of Southampton clearly set out key information about how to manage research data. The sections on 'Planning,' 'Storing Your Data,' 'Data and the GDPR' and 'Sharing Your Data' are particularly helpful.