Research Data Management Policy and Procedures

1. Purpose and scope

1.1 This policy provides part of the supporting framework to deliver AECC University College's (AECC UC) commitment to ensuring that those involved in research activities under the University College's auspices are well-informed and compliant with current legal, regulatory, and institutional principles and expectations when planning, conducting, and disseminating their work. AECC UC recognises research data is a valuable institutional asset, and the role of robust research data management in underpinning institutional strategic development, essential functions, and research integrity.

1.2 Good practice in research data management enables AECC UC and its researchers to meet the standards and responsibilities set out in the University College's Code of Good Research Practice [*add link once available*] and to meet funder, ethical, legal and other responsibilities. It is also essential for enabling and safeguarding the longevity and continuing intelligibility of research data.

1.3 AECC UC embraces the international drive towards open science and is committed to developing a research culture that facilitates the advancement and dissemination of knowledge for the public good. Recognising that outputs of University research are a public good, produced in the public interest and for societal benefit, AECC UC embraces the Concordat on Open Research Data and the UKRI Common Principles on Research Data. Making AECC UC research data freely accessible, wherever this is appropriate, ensures that a wide range of audiences can freely discover, engage, and reuse its research. This is beneficial to our researchers, AECC UC as an institution, academia, and society.

1.4 The policy sets out the support and guidance that researchers should follow to enable them to promote good practice in research data management, to foster responsibility for data management, and to ensure the sharing of eligible research data with as few restrictions as possible, while at the same time respecting concerns in relation to privacy, safety, security and commercial interests.

1.5 The policy aims to ensure that research data is:

- stored in a secure and safe manner;
- identifiable, retrievable and available when needed (and as appropriate);
- an accurate, complete, authentic, reliable and coherent representation of the materials used/collected;
- kept in a manner that is compliant with legal and ethical obligations, AECC UC policy and, where applicable, the requirements of funding bodies;
- able to be made available to others in line with appropriate ethical, data sharing, FAIR (Findable, Accessible, Interoperable, and Reusable) and open access principles.

1.6 This policy applies to AECC UC staff, postgraduate research students, and those associated with the university such as visiting fellows and visiting professors (henceforth referred to as 'researchers'). All researchers must adhere to their obligations under this Policy.

1.7 The policy does not normally apply to taught postgraduate and undergraduate students, except in exceptional circumstances, including, but not limited to, where research findings are included in published research outputs.

1.8 All researchers create some type of data as part of the research data lifecycle. Research data refers to the recorded information (regardless of the form or the media in which it may exist) necessary to support or validate a research project's observations, findings or outputs. Along with research publications, research data forms an important part of the scholarly record.

1.9 As part of a commitment to research excellence, AECC UC seeks to promote the highest standards in the management of research data throughout the research data lifecycle. As such, research data will be managed in accordance with this and with the University College's other policies and guidelines including:

- Code of Good Research Practice [*add link once available*]
- Research Ethics Policy & Procedures
- Data Protection Policy
- Privacy Notice – Research Participants
- Publications & Open Access Policy & Procedures
- Research Misconduct Policy & Procedures
- Research Data Sharing Agreement [*add link once available*]
- IT Acceptable Use Policy
- Data Protection Breach Policy

1.10 Guidance and support for research data management is available from the AECC UC RKE Hub: https://aeccacuk.sharepoint.com/sites/Researchknowledgeexchange/SitePages/Research-Data-Management.aspx.

1.11 The Research Team (research@aecc.ac.uk) can help with queries about research data management. In addition, the Data Protection Officer (dpo@aecc.ac.uk) can be contacted with questions at any time around data protection and storage.

1.12 The deliberate or reckless mismanagement of research data and/or primary materials constitutes unacceptable research conduct and should be reported in line with AECC UC's Research Misconduct Policy & Procedures.

2. Researcher responsibilities

General:

2.1 Principal Investigators and project leads have overall responsibility for effective data management during research projects. However, all researchers have a personal responsibility to effectively manage the research data generated within or obtained from their research and must act in accordance with this policy.

2.2 Responsibility for ensuring the effective day-to-day management of research data lies with the researcher. This includes understanding and complying with any provisions regarding the ownership, preservation and dissemination of research data of research contracts with or grants to the University College.

Data management plans:

2.3 In line with good practice, researchers are strongly encouraged to routinely prepare, maintain, and adhere to a data management plan for their research projects. Data management plans should address the capture, management, integrity, confidentiality, retention, ownership, sharing and publication of research data, including compliance with relevant legal and ethical frameworks. Plans must also adhere to any funder requirements where these exist. Links to guidance and examples of data management plans are available on the RKE Hub.

Externally funded and collaborative research:

2.4 Researchers will identify the resources required to effectively manage research data and will seek, where possible, to recover the direct costs of managing research data and any work needed to make the data available for sharing from their research funder. This is particularly relevant where research data management plans identify additional costs such as extra storage, long-term retention, or significant data management effort.

2.5 Where research is conducted in collaboration with external research partners, researchers must ensure that suitable agreements for the ownership and use of research data are prepared and agreed in writing by the parties concerned before the project starts. This should also cover the rights and responsibilities of each party regarding how the data will be collected, including key decisions about data storage, backup and security, registration, access, transfer, retention, destruction or archiving, and licensing. Help, guidance and template agreements are available from the Research Team.

Data collection, processing and analysis:

2.6 Researchers must be aware of their and the University College's legal obligations and potential liability when processing data relating to people to ensure compliance with handling data protected by the UK Data Protection Act (2018) and the European Union General Data Protection Regulation (2016), together with any other applicable data protection or privacy laws). Researchers will protect confidential, personal, and sensitive research data in accordance with legal and ethical requirements related to the research they conduct. Legal, ethical and commercial constraints on the sharing of research data must be considered at the initiation of the research process and throughout the research data lifecycle and will normally be described in a data management plan.

Data loss or security breach procedure:

2.7 There are potentially significant repercussions for the University College and the individuals affected arising from a data loss or security breach. Where this occurs or you suspect it may have occurred, you must follow the guidance provided in the University's Data Protection Breach Policy:

- It is important that this is done immediately, as it may be possible to reduce the impact of the breach by remote deletion, removal or other means.
- Follow their guidance on dealing with the security breach and keep the Data Protection Officer up to date with any further information about it that you become aware of.
- Do not approach any individual data subjects, suppliers, regulators or make any public announcements about the security breach incident without the prior agreement of the Data Protection Officer.

Data storage, access and sharing:

2.8 Researchers must ensure that all research data in digital and computer-readable form:
- is stored securely in a durable format appropriate for the type of research data in question;

- is stored with adequate metadata and/or documentation to facilitate identification and support effective reuse of research data where this is appropriate;
- is backed-up regularly in accordance with best practice in the relevant field of research.

2.9 Researchers must ensure that all non-digital research data that is unsuitable for digitisation, but which is significant should be (see clause 5.4 for a definition of non-significant research data):

- stored securely;
- labelled, indexed or categorised appropriately to identify the research data in question and support effective reuse of research data where this is appropriate.

2.10 Before sharing research data during or after a project, researchers must determine whether this is permissible considering data sharing restrictions, intellectual property rights (IPR) ownership, ethical, privacy, confidentiality requirements or any legal, regulatory or funding restrictions. In addition, researchers must consider whether research data has commercial potential and in consultation with the Research Team consider if it is suitable for IP protection and/or transfer.

2.11 If, after considering clause 2.9, it is deemed appropriate to share the research data, researchers should offer the research data they have selected for preservation and sharing to an appropriate data repository, along with sufficient descriptive metadata and documentation to ensure that it can be found and understood. AECC UC does not yet have an institution repository for research data. However, external data repositories are available (the Research Team can advise on this and information is available on the RKE Hub). Also, if the research is a collaboration with another university, the other university may have an institutional data repository to which the data could be uploaded.

2.12 Researchers must include a data access statement in their published research outputs which clearly describes how and on what terms any supporting data may be accessed. See Section 3.1 of the AECC UC Publications & Open Access Policy & Procedures for guidance.

2.13 Researchers are encouraged to obtain an ORCID identifier to help them record and report their work. This identifier can be used in publications, grant applications, funder reporting and impact tracking.

2.14 Technicians, professional, and support staff instrumental in contributing to the collection and/or generation of research data should be acknowledged, and their contribution specified in descriptive metadata and in data access statements.

Data disposal:

2.15 Researchers must securely dispose of research data identified for deletion or destruction, in accordance with legal, ethical, research funder and collaborator requirements and with particular concern for the confidentiality and security of the data. The agreed processes for the timing, manner and recording of research data disposal and destruction should be included in the research data management plan and stored with other project information and documentation. Data disposal must be carried out in accordance with AECC UC's Data Protection Policy.

Postgraduate research students:

2.16 The University College believes that embedding research data management practice in early career researchers is critical to establishing an effective data management ethos. Therefore, where research is undertaken by postgraduate researchers, it is the responsibility of the staff member supervising their project to ensure that the postgraduate researcher has a clear understanding of

their research data management responsibilities and engages with training and development as necessary. Supervisors should work with the postgraduate researcher to determine which research data is selected for archiving and sharing and to decide an appropriate route to achieve this. All postgraduate researchers should produce and maintain a research data management plan.

3. Manager responsibilities

3.1 The Heads of School, School Research Leads and other staff responsible for research staff and students are responsible for promoting good practice in all aspects of research governance and integrity including research data management. They should ensure that staff and students are aware of this policy and their responsibilities and obligations in effective management of research data. They should also identify or promote training where gaps in these skills are identified.

3.2 Heads of School/equivalent assume stewardship of data once the researchers involved in compiling the data leave the University College. They must work with the researcher to agree how research data will be located and how it will be stored. This role may be delegated to a dedicated data steward or stewards to act as custodian of such data on the University College's behalf until it is destroyed.

4. University responsibilities

4.1 The University College acknowledges its obligations under research funders' data policies and codes of practice to ensure that sound systems are in place to promote and reinforce good practice in research data management.

4.2 The University College is committed to providing:

- researchers with access to training, support, advice and information on all aspects of research data management;
- guidance on accessing services and facilities for the storage, backup, registration, deposit and discovery of research data;
- the necessary resources to enable the provision of these services, facilities and training.

5. Data retention periods

5.1 Subject to clause 5.2, all research data which is stored in accordance with this policy should be held for a minimum period of 10 years from collection, creation or generation of the research data or publication of the research results (whichever is the later) provided appropriate safeguards are in place to protect any personal data necessary to achieve the research objectives contained within it.

5.2 Research data will be retained for longer than ten years:

- where an increased retention period is required to meet the University's statutory obligations, contractual obligations or the guidelines of the body funding the relevant research project;
- where the results of the research have resulted in a patent application;

- where the results of the research become contentious or subject to challenge at any time during the initial 10-year retention period, in which case Research Data should be retained pending review and not destroyed or otherwise disposed of until the matter is fully resolved.

5.3 Research data may be retained for longer than ten years where the research has a public interest or heritage value.

5.4 Research data that is not deemed 'significant' data need not be retained beyond the end of the research project. Non-significant data could include early research notes, early versions of later documents, or material which is expensive to store but quick and easy to collect again. Unless a publication is planned from the research, all research data resulting from work undertaken by taught undergraduate and postgraduate students towards their dissertations would fall into this category and need not be retained after the degree has been awarded.

6. Good practice

6.1 In drafting this policy and procedure, good practice has been adopted from other universities including:

- University of Edinburgh: https://www.ed.ac.uk/information-services/about/policies-and-regulations/research-data-policy
- University of Northampton: https://www.northampton.ac.uk/wp-content/uploads/2021/04/research-data-management-policy.pdf
- University of Southampton: https://www.southampton.ac.uk/about/governance/regulations-policies/policies/research-data-management
- University of Surrey: https://www.surrey.ac.uk/sites/default/files/2022-06/research-data-management-policy_0.pdf
- University of York: https://www.york.ac.uk/staff/research/governance/research-policies/research-data-management-policy/
- University of Winchester: https://www.winchester.ac.uk/media/critical-documents/Research-Data-and-Records-Management-Policy.pdf

7. Further guidance

7.1 Further guidance on research data management is available from:

- AECC UC RKE Hub: https://aeccacuk.sharepoint.com/sites/Researchknowledgeexchange/SitePages/Research-Data-Management.aspx
- Digital Curation Centre: https://www.dcc.ac.uk/
- UK Data Service: https://ukdataservice.ac.uk/learning-hub/research-data-management/
- JISC's Research Data Management Toolkit: https://www.jisc.ac.uk/guides/research-data-management-toolkit
- UK Reproducibility Network: https://www.ukrn.org/

Approved by	Endorsement: Research & Innovation Committee
	Approval: Academic Board
Originator/Author	Research Team
Owner	Head of Research
Reference source	Exemplars from the HE Sector
Date approved	June 2024
Effective from	01 July 2024
Review date	April 2025
Target	AECC University College staff and students conducting research (this includes visiting fellows/professors)
Policy location	Staff Information Portal (SIP)
Equality analysis	This Policy has been developed with due regard to the University College's general equality duty and no direct impact has been identified.