Plan Overview

A Data Management Plan created using DMPonline

Title: International regulatory framework of maritime cybersecurity and enhancement of human element

Creator: Jihyeon Gina Kim

Principal Investigator: Jihyeon Gina Kim

Contributor: Kimberly Tam

Affiliation: University of Plymouth

Template: DCC Template

ORCID iD: 0009-0001-2410-0394

Project abstract:

This project investigates how a future international maritime cybersecurity code under the International Maritime Organization (IMO) could enshrine human element principles from the very outset of its development. Despite longstanding recognition that effective maritime safety depends on a holistic understanding of the human element, current regulatory approaches remain predominantly technical, overlooking the human, organisational, and cultural dimensions essential to cyber resilience.

Through interviews with IMO member state representatives, industry partners, and key stakeholders, the project aims to identify how human element considerations can be systematically embedded into the regulatory design process, and to evaluate current levels of awareness and readiness among key actors. Field observations at IMO meetings and industry events will further inform the research findings.

A central focus of the project is the role of ownership and collective responsibility in strengthening maritime cyber resilience. Story sharing — through the exchange of incidents, lessons learned, and best practices — is explored as a key mechanism for cultivating accountability and cooperation, addressing the fragmentation that has long hindered transparent and collaborative cyber risk management across the industry.

The project will ultimately propose directions for a mandatory international maritime cyber code that embeds human element principles throughout all levels of cyber risk management, establishing a coherent, human-centred regulatory framework to safeguard life, property, and the marine environment in the digital era.

ID: 203679

Start date: 15-09-2025

End date: 15-09-2026

Last modified: 07-05-2026

Copyright information:

International regulatory framework of maritime cybersecurity and enhancement of human element

Data Collection

What data will you collect or create?

Data Description

This project will collect and create three categories of data: primary qualitative data generated through interviews and field observation, and secondary data gathered through a desktop study.

Interview recordings will be captured as audio/video files via Microsoft Teams (.mp4 format), with an estimated volume of approximately 500MB-1GB in total across all interviews. Transcripts derived from recordings will be stored as Microsoft Word documents (.docx) and plain text files (.txt), estimated at a total of 50-100MB. Field notes will be created and stored as .docx files, estimated at under 10MB. Secondary data will consist of existing publicly available documents in .pdf format, estimated at 100–200MB. The overall estimated total data volume is therefore under 2GB, which poses no significant challenges for storage, transfer, or preservation on the University of Plymouth's institutional OneDrive.

Data Formats and Justification

Microsoft Teams (.mp4) is used for recordings as it is the platform through which interviews will be conducted, ensuring compatibility and ease of access. Word (.docx) and plain text (.txt) formats are widely used, non-proprietary in practice, and supported by long-term archiving standards. PDF is the standard format for regulatory and official documents and ensures formatting integrity. These formats are consistent with UK Data Service recommendations for long-term usability, sharing, and archiving, and do not require specialist software to access.

Existing and Third-Party Data

A substantial body of existing data will be reused through the desktop study, including publicly available IMO and UN regulatory instruments, official industry guidance documents, and peer-reviewed academic literature. All such materials are publicly accessible and no copyright or intellectual property restrictions apply to their use for academic research purposes. These materials will complement and contextualise the primary data collected through interviews and field observation, enabling methodological triangulation across all three data sources.

Long-Term Value

Anonymised interview transcripts and field notes are considered to be of long-term value and will be retained for a minimum of 10 years post-project in accordance with the University of Plymouth Research Data Policy. Raw interview recordings will be deleted following transcription, participant verification, and dissertation submission, in line with the data minimisation principle under UK GDPR. Secondary documentary materials are publicly available and do not require long-term preservation by this project.

How will the data be collected or created?

Primary data will be collected using semi-structured interviews, following established qualitative research methodology. Interview questions have been developed and reviewed by the academic supervisor to ensure consistency, neutrality, and alignment with the research aims. Thematic analysis will be applied to interview transcripts following the framework of Braun & Clarke (2006), a widely recognised and documented methodology for qualitative data analysis. Field notes will be structured around key themes identified during the interview phase, ensuring systematic and consistent

recording across observation events.

Folder Structure

All data will be organised on the supervisor's secure University of Plymouth OneDrive using the following folder structure:

International regulatory framework of maritime cybersecurity and enhancement of human element
  Interview invitations/
  Interview consent forms/
  Interview_Recordings/
  Interview_Transcripts/
    Field_Notes/
  Dissertation_Drafts/
    Analysis/
    Outputs/
    Desktop_Study/
    Regulatory_Documents/
    Industry_Guidance/
    Academic_Literature/
  Delivery_Presentation

File Naming Convention

All files will follow a consistent naming convention:

[DataType]_[ParticipantCode/FieldNoteCode]_[Version]

For example:

- Appendix_Redacted_Interview_P01_amended
- Full Transcript_Interview_P01
- Field Note_1_correction

Version Control

Document versioning will be managed through Microsoft OneDrive's built-in version history function, which automatically tracks and stores previous versions of files. Major revisions will be only indicated by type of edit carried out in the filename (e.g. amended, correction).

Quality Assurance

The following quality assurance processes will be applied throughout the project:

- Interview questions reviewed and approved by the academic supervisor prior to data collection
- All AI-generated transcripts manually reviewed and corrected by the principal investigator to ensure accuracy, with particular attention to maritime cybersecurity terminology
- Transcripts shared with participants for member-checking, allowing participants to review and correct their own transcript, to enhance the accuracy and credibility of the data
- Field notes reviewed and consolidated by the principal investigator within 24 hours of each observation event to ensure completeness
- Thematic analysis reviewed by the academic supervisor to verify consistency and rigour of interpretation
- All data collection conducted in accordance with the University of Plymouth Research Ethics Policy (PEOS Reference No: 6782) and UK GDPR

Documentation and Metadata

What documentation and metadata will accompany the data?

Information required for interpretation

To ensure the data can be read and interpreted in the future, the following documentation will accompany the dataset:

- Methodological Framework: A copy of the semi-structured interview guide, which outlines the five core thematic areas: Stakeholder Dimension, Goals and Objectives, Functional Requirements, Evaluating the Progress, and Closing Reflections.
- Contextual Definitions: The specific definition of the "human element" as used in this project, which is based on IMO Resolution A.947(23).
- Procedural Information: Documentation of the data collection process, including the pre-interview announcement, the use of verbal and written consent, and the fact that interviews were recorded and transcribed for analysis.
- Variable Definitions: Definitions of demographic variables collected, such as organisation type (Member State/Industry/International Organisation), geographical location, and maritime industry experience.

Capture and creation of documentation

- Transcription and Review: Initial transcripts are created via recording software and then manually corrected for accuracy,. Participants are given the opportunity to review and provide final agreement on the transcripts before they are used for analysis.
- Redaction and Anonymisation: To comply with the University of Plymouth’s research ethics policy (PEOS Reference No: 6782) and UK GDPR, a redacted version of each transcript is created. This process involves replacing personally identifiable information (PII) with non-identifiable descriptors (e.g., [REDACTED: organisation]).
- Recording of Information: Metadata and documentation will be recorded in 'readme' text files accompanying the data files and within the file headers of the transcript documents themselves.

Metadata standards

While the sources do not specify a specific community standard, the metadata provided will follow standard academic repository requirements to ensure discoverability:

- Administrative Metadata: Creator (Jihyeon Gina Kim), title of the project, date of creation (e.g., 26 November 2025), and version history (e.g., unredacted vs. redacted).
- Access Conditions: Clearly defined conditions under which the data can be accessed, noting that unredacted recordings are securely stored on encrypted devices accessible only to the Principal Investigator, while redacted transcripts are available for broader research compliance.

Documentation for data reuse

To enable secondary users to reuse the data effectively, the following will be provided:

- File Formats: Data is primarily stored in Microsoft Word (.docx) format for ease of text analysis.
- Analytical Notes: Information on any assumptions made during the interview process, such as the participant's role in "loss prevention" or their organisation's status as a "non-profit mutual insurance club".
- Demographic Context: A summary of the participant's background, including their involvement in IMO instruments (e.g., ISM, ISPS, and STCW Codes) to provide context for their insights.

Ethics and Legal Compliance

How will you manage any ethical issues?

The project demonstrates proactive ethical planning by integrating the "review and final agreement" phase, which ensures that participants maintain agency over their data throughout the research lifecycle. This approach aligns with the University of Plymouth's ethical standards, ensuring that the "human element" of the research is handled with the same level of security and respect advocated for in the maritime industry itself.

Consent

- Informed Multi-Stage Consent: Consent is obtained through a formal interview consent form and a verbal confirmation recorded at the start of each session. Participants are informed that the data will be used for analysis and that the resulting transcripts will be shared with them for review and final agreement before being formally processed.
- Explicit Sharing Permissions: Rather than promising immediate deletion, the protocol ensures participants are aware that the final agreed transcripts will be preserved for the project's duration and potentially shared in a redacted format. Additionally, explicit consent is sought for public acknowledgments, such as naming participants on professional platforms like LinkedIn upon project completion.

Protection of participant identity

- Redaction and Anonymisation: To comply with the UK GDPR and the University of Plymouth Research Ethics Policy (PEOS Reference No: 6782), a robust redaction strategy is employed,. All personally identifiable information (PII) is removed from shared datasets, including:
  - Names of individuals (interviewees and colleagues).
  - Names of specific organisations and agencies.
  - Specific geographical identifiers (cities, specific office locations).
  - Contact information and email addresses.
- Use of Descriptors: To maintain the research's contextual value, PII is replaced with non-identifiable descriptors (e.g., *[REDACTED: organisation]* or *[REDACTED: participant name]*). Participants are given the opportunity to review these redacted versions to confirm they are satisfied with the level of anonymisation and institutional compliance.

Handling of sensitive data

- Secure Storage: All sensitive data, including unredacted audio recordings and original transcripts, are stored exclusively on encrypted devices.
- Managed Access: Access to raw, unredacted data is strictly restricted to the Principal Investigator (PI).
- Secure Transfer: Transcripts are shared with participants for verification purposes to ensure transparency regarding the data being used,. By using a redacted format for the broader research database, the project minimizes the risk of accidental disclosure of sensitive professional or personal information.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

Data ownership

- Primary Ownership: The University of Plymouth and the Principal Investigator (PI), Jihyeon Gina Kim, hold the primary copyright and IPR for the original research data generated, including interview recordings, transcripts, and the final analytical dataset.
- Participant Contributions: While the university owns the research outputs, participants retain rights to the specific professional insights provided during the interview until they give "final

agreement" on the corrected transcript. Data is only formally incorporated into the project's dataset once this participant-level clearance is obtained.

Licensing for reuse

- Redacted Transcripts: The redacted versions of the transcripts, which comply with UK GDPR and institutional ethics policies, are intended for preservation and potential reuse. These will likely be made available under a standard academic license, to ensure the researcher is credited while allowing secondary analysis.
- Unredacted Data: Access to raw audio and unredacted transcripts remains restricted and is not licensed for public reuse to protect the privacy and professional standing of the interviewees.

Restrictions on third-party data

- Participant-Provided Materials: During the research process, some participants may share third-party materials, such as internal presentations or proprietary slides.
- Management of Third-Party Rights: The IPR for such materials remains with the participant's organisation. These materials are used strictly for contextual analysis within the project and are not shared or republished without explicit secondary permission from the original copyright holders.

Postponement and restrictions on sharing

- Embargo for Publication: Data sharing is restricted until the project is finalised in September 2026. This allows for the completion of the research analysis and ensures any associated publications are secured before the underlying data is made available.
- The "Review and Agree" Restriction: A permanent restriction exists where data cannot be shared or used unless the participant has reviewed the transcript and provided a "thumbs up" or final agreement.
- Ethical Redaction: Sharing is permanently restricted to redacted formats only; unredacted data is stored on encrypted devices and will not be shared publicly to maintain compliance with University of Plymouth Research Ethics Policy (PEOS Reference No: 6782).

Storage and Backup

How will the data be stored and backed up during the research?

All primary research data, including unredacted recordings and interview transcripts, are securely stored on encrypted devices that are accessible only to the Principal Investigator. To ensure data security and protect sensitive personally identifiable information (PII), the project utilises redaction and anonymisation for any shared versions of the data, such as removing the names of individuals, organisations, and specific geographical identifiers.

The research is conducted in strict accordance with the UK General Data Protection Regulation (UK GDPR) and the University of Plymouth Research Ethics Policy (PEOS Reference No: 6782).

Responsibility: The Principal Investigator is the sole individual responsible for managing the encrypted devices where the unredacted data is held.

Data Retention: In line with data protection agreements made with participants, identifying data and recordings will be discarded and deleted after three years.

Transcription Processes: Transcription is initiated through managed digital services, as evidenced

by the time-stamped logs, and shared with participants for review before final agreement and redaction.

The project utilises the University of Plymouth's institutional Microsoft 365 account, which provides 1TB of OneDrive storage, significantly exceeding the estimated 2GB data volume of this project. No additional storage costs are required. Files saved to OneDrive are automatically synced and backed up continuously, with version history retained for up to 180 days, enabling file recovery in the event of accidental deletion or modification.

As this project is planned for completion within one year, data will remain on the principal investigator's University of Plymouth OneDrive throughout the active research phase. Prior to the expiry of the university account upon graduation, all data will be reviewed and, if required for continued research purposes such as progression to a PhD, transferred to the academic supervisor's University of Plymouth OneDrive before account closure. This transfer will be agreed with the academic supervisor in advance of the account expiry date. If no further research use is required, anonymised data of long-term value will be retained in accordance with the university's 10-year data retention policy through an agreed institutional storage solution.

How will you manage access and security?

Data collected in this project is classified as Confidential prior to anonymisation, as it contains personally identifiable information (PII) relating to interview participants. The primary security risks identified are unauthorised access to participant data, accidental data loss or deletion, and potential data breach during transfer. These risks are managed through the measures outlined below.

Access Control

Access to all research data is restricted to the principal investigator and academic supervisor only. Data is stored on the University of Plymouth's institutional OneDrive, which is protected by the university's Microsoft 365 authentication system, including multi-factor authentication (MFA). No research data will be shared with third parties except where participants request sight of their own transcript for verification purposes, in which case only their individual anonymised transcript will be shared via encrypted email.

Data Security Measures

The following security measures are in place throughout the project:

- All data stored on the University of Plymouth's institutional OneDrive, managed and secured by university IT Services in accordance with institutional information security policies
- Multi-factor authentication applied to all Microsoft 365 account access
- No personally identifiable data entered into third-party AI tools or unsecured platforms
- AI transcription tools confirmed as UK GDPR-compliant by University of Plymouth IT Support (TIS)
- All devices used to access research data password-protected
- Anonymisation applied at the point of transcription, with participants assigned pseudonyms and all identifying information removed

Field Data Transfer

During field study attendance at IMO meetings and industry events, field notes will be recorded directly into a password-protected device. Notes will be transferred to the University of Plymouth OneDrive at the earliest opportunity following each event, and no field data will be retained solely on a personal device beyond the point of transfer. Where events are attended internationally, transfer will be completed upon return to a secure internet connection.

Collaborator Access

This project does not involve external collaborators requiring access to raw data. The academic supervisor has access to research data via the University of Plymouth's institutional OneDrive. No data will be shared via unsecured channels.

Formal Standards and Institutional Policies

All data management and security practices comply with:

- UK General Data Protection Regulation (UK GDPR)
- University of Plymouth Research Ethics Policy (PEOS Reference No: 6782)
- University of Plymouth Information Security Policy
- ISO 27001 principles for information security management, as applied through the university's institutional IT infrastructure

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Data to be Retained

The following data are considered to be of long-term value and will be retained for a minimum of 10 years from the date of dissertation submission or publication of findings, whichever is the later, in accordance with the University of Plymouth Research Data Policy:

- Anonymised interview transcripts: These constitute the primary evidence base underpinning the research findings and are of potential value for future research into maritime cybersecurity governance, human element integration, and international regulatory development
- Field notes: Observations recorded at IMO meetings and industry events provide a contemporaneous account of international policy discourse that may be of value for longitudinal research in this field
- Final analysis files and dissertation: The processed outputs of the research, including thematic analysis findings, are retained to enable validation of research findings and support future academic or policy work

Data to be Destroyed

The following data will be destroyed upon completion of their immediate purpose:

- Raw interview recordings: Deleted following transcription, participant verification, and dissertation submission, in line with the data minimisation principle under UK GDPR and participant consent agreements
- Secondary documentary materials: Sourced entirely from publicly available sources and therefore not retained by this project, as they remain openly accessible to future researchers independently

Legal and Regulatory Obligations

All data retention and destruction decisions comply with UK GDPR, the University of Plymouth Research Ethics Policy (PEOS Reference No: 6782), and the University of Plymouth Research Data Policy. No contractual obligations from external funders apply to this project.

Foreseeable Research Uses

The retained anonymised data has foreseeable value for:

- Validating and replicating the findings of this dissertation
- Informing future research into the completion of a non-mandatory IMO Cyber Code
- Supporting longitudinal studies tracking the evolution of international maritime cybersecurity governance
- Potential use in teaching and training contexts related to maritime cybersecurity policy and

human factors
- Informing policy development at the IMO and within member state administrations

What is the long-term preservation plan for the dataset?

Data Selection for Long-Term Preservation

Not all data collected during this project is of equal long-term value. The following distinctions apply:

- Retained for 10 years: Anonymised interview transcripts, field notes, and final analysis files, as these directly underpin the research findings and may be of value for future maritime cybersecurity policy research
- Deleted upon project completion: Raw interview recordings, once transcripts have been verified by participants and the dissertation submitted, in line with the data minimisation principle under UK GDPR
- Not retained beyond project: Secondary documentary materials sourced from publicly available sources, as these remain openly accessible and do not require preservation by this project

Repository and Archive

Given the qualitative and policy-oriented nature of this project, anonymised data of long-term value will be deposited in the University of Plymouth's institutional research data repository upon completion of the dissertation. This ensures the data is preserved, discoverable, and managed in accordance with the university's Research Data Policy beyond the lifetime of the project.

Should the research lead to a published output, data will additionally be made available in accordance with the relevant journal or publisher's open data requirements. In the event of progression to a PhD, data will be transferred to the academic supervisor's University of Plymouth OneDrive prior to the expiry of the principal investigator's university account, as agreed with the supervisor.

Costs

The University of Plymouth's institutional repository is available at no additional cost to researchers. No external repository charges are anticipated. The primary cost associated with long-term preservation is the time required to prepare data for deposit. Rather than a standalone task, data preparation is an ongoing activity integrated throughout the 12-month project, encompassing the consistent application of naming conventions, folder organisation, anonymisation procedures, and metadata documentation from the outset of data collection. A final review and quality check of all retained data will be carried out by the principal investigator prior to dissertation submission to confirm readiness for deposit.

Data Preparation for Deposit

Prior to deposit, all retained data will be:

- Reviewed to confirm full anonymisation, with all participant pseudocodes checked against the master participant log
- Organised in accordance with the folder structure and file naming conventions established at the outset of the project
- Accompanied by the project README file and metadata log, ensuring the data is fully documented and interpretable by future users
- Converted to open, non-proprietary formats where appropriate, specifically, transcripts will be saved as plain text (.txt) in addition to .docx, in line with UK Data Service recommendations for long-term usability

Retention Period

In accordance with the University of Plymouth Research Data Policy, all retained data will be preserved for a minimum of 10 years from the date of dissertation submission or publication of findings,

whichever is the later.

Data Sharing

How will you share the data?

Approach to Data Sharing

Given the confidential and sensitive nature of participant contributions, data sharing will be managed carefully and proportionately. All shared data will be fully anonymised prior to release, with no personally identifiable information disclosed. Raw interview recordings and full transcripts will not be shared under any circumstances.

With Whom and Under What Conditions

Data will be shared in the following ways:

- Dissertation appendices: Summarised versions of redacted interview transcripts will be appended to the final dissertation as evidence of research ethics compliance, accessible to the dissertation examination committee and, upon approval, through the University of Plymouth's institutional repository
- Academic publication: Should findings be published in academic journals or conference proceedings, supporting anonymised and summarised data will be made available in accordance with the relevant publisher's open data requirements
- IMO presentation: Subject to dissertation approval, findings may be presented at the International Maritime Organization (IMO) headquarters. Aggregated and anonymised findings only will be shared in this context; no individual transcript or participant-level data will be disclosed
- Future researchers: Summarised redacted transcripts and field notes deposited in the University of Plymouth's institutional repository will be accessible to future researchers, subject to any access conditions applied at the point of deposit

Repository and Discovery

Retained data will be deposited in the University of Plymouth's institutional research data repository upon dissertation submission. A persistent identifier (DOI) will be sought for the dataset at the point of deposit, enabling reliable discovery, citation, and tracking of reuse. Metadata will be made publicly available in accordance with the metadata standards recommended by the University of Plymouth's institutional repository, ensuring the dataset is findable and interpretable by future users.

Timing of Data Release

Data will be made available upon dissertation submission and institutional approval. An embargo period of up to 36 months from submission will be applied to protect the integrity of planned academic publication arising from the research, and to accommodate the possibility of progression to a PhD built upon these findings. Given the uncertainty around academic publication timelines and the potential for continued research use, this extended embargo period is considered necessary and proportionate. No prolonged exclusive use beyond this period is anticipated, and the embargo will be lifted at the earliest opportunity should publication and any subsequent research progression be concluded sooner.

Are any restrictions on data sharing required?

Access Restrictions

Access to the deposited dataset will be subject to the following conditions, reflecting the sensitivity of

the data and participant consent agreements:

- Data will be available for academic research, educational purposes, and providing supporting information for regulatory development only
- Users will be required to acknowledge the source of the data in any publication or output arising from its reuse
- Any request to use the data for commercial purposes will be referred to the principal investigator and academic supervisor for consideration

Minimising Restrictions

Restrictions on sharing have been minimised through the following strategies applied throughout the project:

- Full anonymisation and summarisation of all transcripts prior to sharing
- Participant consent obtained in advance, including consent for anonymised data to be used and retained beyond the immediate project
- Use of open, non-proprietary file formats (.txt, .docx) to facilitate access and reuse
- Consistent application of the metadata standards recommended by the University of Plymouth's institutional repository to ensure discoverability
- A time-limited embargo rather than permanent restriction, ensuring data becomes openly accessible at the earliest appropriate opportunity

Responsibilities and Resources

Who will be responsible for data management?

This is an independently conducted research project with no external collaborators or partner institutions. Data management responsibilities are shared between the principal investigator and academic supervisor as follows:

Principal Investigator

Jihyeon Gina Kim MRes Maritime Cyber Security, School of Science and Engineering, University of Plymouth Email: jihyeongina.kim@postgrad.plymouth.ac.uk

The principal investigator holds primary responsibility for the day-to-day implementation of this Data Management Plan, including:

- Data capture; conducting interviews, recording field notes, and collecting desktop study materials
- Metadata production; maintaining the project README file, file-level documentation, and metadata log throughout the project
- Data quality; manually reviewing and correcting all AI-generated transcripts, conducting member-checking with participants, and ensuring consistency of file naming and folder organisation
- Anonymisation; applying pseudocodes to all participants and removing identifying information at the point of transcription
- Storage and backup; uploading all data to the supervisor's secure University of Plymouth OneDrive promptly following collection, and maintaining the secondary encrypted USB backup updated fortnightly
- Field data transfer; transferring field notes to the OneDrive at the earliest opportunity following each observation event
- Data preparation for deposit; organising, reviewing, and formatting all retained data for deposit in the University of Plymouth's institutional repository prior to dissertation submission
- DMP review and revision; reviewing and updating this Data Management Plan in consultation with

the academic supervisor as the project progresses

Academic Supervisor

Dr Kimberly Tam School of Science and Engineering, University of Plymouth Email: kimberly.tam@plymouth.ac.uk

The academic supervisor holds supervisory responsibility for data management, including:

- Providing access to the secure University of Plymouth OneDrive for primary data storage throughout the project
- Reviewing and approving interview questions and data collection procedures to ensure compliance with research ethics requirements
- Overseeing the quality and rigour of thematic analysis to ensure consistency of interpretation
- Supporting the principal investigator in ensuring compliance with UK GDPR, the University of Plymouth Research Ethics Policy (PEOS Reference No: 6782), and the University of Plymouth Research Data Policy
- Reviewing and approving this Data Management Plan
- Agreeing and facilitating the transfer of data to the supervisor's OneDrive in the event of PhD progression prior to the expiry of the principal investigator's university account

What resources will you require to deliver your plan?

This project is modest in scale and does not require significant additional resources beyond those already available through the University of Plymouth's institutional infrastructure. The following resources have been identified:

Storage and IT Infrastructure

- University of Plymouth institutional Microsoft 365 account, providing 1TB of OneDrive storage, already available at no additional cost
- Microsoft Teams for conducting and recording interviews, already available through the university's Microsoft 365 subscription at no additional cost
- AI transcription tools confirmed as UK GDPR-compliant by University of Plymouth IT Support (TIS), already available through the university's Microsoft 365 subscription at no additional cost
- Encrypted, password-protected USB drive for secondary backup, already in possession of the principal investigator at no additional cost

No additional hardware or software beyond existing institutional provision is required for this project.

Software

- Microsoft Word (.docx) for transcript and field note documentation, already available through the university's Microsoft 365 subscription
- Plain text editor (.txt) for open-format file copies, freely available
- University of Plymouth institutional research data repository for long-term deposit, available at no additional cost to researchers

No charges will be applied by the University of Plymouth's institutional data repository. No external repository is required for this project.

Training and Expertise

The principal investigator has completed, or will complete prior to data collection, the following training to ensure competent delivery of this Data Management Plan:

- University of Plymouth research data management training, available through the Researcher Development Programme
- University of Plymouth research ethics training in accordance with PEOS requirements

- Familiarisation with UK GDPR obligations as they apply to qualitative research data, through institutional guidance provided by the university

No additional specialist technical expertise is required beyond that available through the university's existing IT support services. Should any technical difficulties arise in relation to data storage, backup, or repository deposit, support will be sought from University of Plymouth IT Services (TIS) and the university library's Information Specialists, both of whom provide dedicated research data management support at no additional cost.

Travel and Field Data Collection Costs

This research is self-funded by the principal investigator. Attendance at IMO meetings and industry events constitutes the field study component of this project and represents the primary data collection activity for observational data. Any travel and admission costs associated with this activity are research project costs borne by the principal investigator and managed separately from this Data Management Plan. As there is no external funder, no additional funder-specific data management requirements apply beyond those stipulated by the University of Plymouth Research Data Policy. No additional data management infrastructure, tools, or services are required to support field data collection beyond those already outlined above.

No additional costs are anticipated for data management, storage, backup, repository deposit, or preservation. This research is self-funded and no external funder requirements apply beyond the University of Plymouth Research Data Policy.