Plan Overview

A Data Management Plan created using DMPonline

Title: Supplier Engagement for Scope 3 Emission Reduction in SME Manufacturing Supply Chains

Creator: Roland Adu-Boffuor

Principal Investigator: Roland Takyi Adu-Boffuor

Contributor: Prof. Jonathan Lean, Prof. Jonathan Moizer, Dr. Minchul Sohn

Affiliation: University of Plymouth

Template: DCC Template

Project abstract:

Small and medium-sized enterprises (SMEs occupy a central position in manufacturing supply chains yet face increasing pressure to address Scope 3 emissions, which predominantly arise from upstream supplier activities beyond their direct operational control. Although prior research highlights the importance of supplier engagement for sustainability, limited attention has been given to how resource-constrained SMEs respond to stakeholder pressures and enact supplier engagement in practice.

This study examines supplier engagement for Scope 3 emissions reduction in SME manufacturing supply chains by integrating Stakeholder Theory and Practice Theory. The research pursues three objectives: (1) to identify the key stakeholder pressures motivating SMEs to engage suppliers on carbon reduction; (2) to explore the strategies SMEs employ to engage suppliers; (3) to examine how such engagement is enacted through everyday organisational routines and practices; (4) to develop a conceptual framework that captures the relationship between stakeholder drivers, engagement strategies, and implementation mechanisms; (5) and to provide both theoretical and practical contributions to the management of Scope 3 emissions in the SME context.

Using a qualitative research design, the study draws on semi-structured interviews with managers in UK manufacturing SMEs and relevant supply-chain actors, supplemented by documentary evidence. A practice-theoretical lens is applied to trace how sustainability commitments are translated into routine procurement activities, interactions, and decision-making processes.

The findings contribute to the literature by moving beyond normative accounts of supplier engagement to reveal the practical mechanisms through which SMEs navigate stakeholder expectations and operational constraints. The study advances understanding of Scope 3 management by highlighting how supplier engagement is shaped by everyday practices rather than formal policies alone. Practically, the results offer insights for policymakers and practitioners seeking to design more context-sensitive supplier engagement approaches that reflect the realities of SME manufacturing environments.

ID: 196623

Start date: 01-10-2024

End date: 30-09-2028

Last modified: 03-02-2026

Copyright information:

Supplier Engagement for Scope 3 Emission Reduction in SME Manufacturing Supply Chains

Data Collection

What data will you collect or create?

This study will generate **qualitative primary data**, supported by **secondary documentary data**, to explore supplier engagement for Scope 3 emissions reduction in SME manufacturing supply chains.

Primary data will be collected through **semi-structured interviews** with key organisational actors within Plymouth Manufacturer's Group, including procurement managers, operations managers, sustainability leads, and senior decision-makers involved in supplier relationships. The interviews will explore perceived stakeholder pressures, supplier engagement strategies, and how engagement is enacted within everyday procurement and operational routines. All interviews will be audio-recorded with informed consent and transcribed verbatim, creating an original qualitative dataset.

Secondary data will consist of organisational and publicly available documents, such as sustainability policies, procurement guidelines, supplier codes of conduct, carbon reporting materials, and relevant regulatory or industry guidance. These documents will be used to contextualise and triangulate interview data.

Data analysis will follow a **thematic analysis approach**, informed by **Practice Theory** and guided by the study's research objectives. Transcripts and documents will be coded iteratively using qualitative data analysis software (e.g. NVivo). Initial open coding will identify recurring patterns related to stakeholder pressures, engagement strategies, and procurement practices. These codes will then be refined into higher-order themes that capture the ways through which supplier engagement is enacted in practice.

How will the data be collected or created?

Primary data will be collected using a qualitative research design, including **semi-structured interviews** and **document collection**.

Participants will be recruited using **purposive sampling**, based on their direct involvement in supplier management and sustainability-related activities.

Initial contact will be made via the Chairman of the Plymouth Manufacturers' Group, email invitations, and industry associations.

Interviews will be conducted either **face-to-face** or **remotely (via Microsoft Teams or Zoom),** depending on participant availability and preference. Each interview will last approximately **45–60 minutes**.

Informed consent:

- In face-to-face interviews, physical copies of consent will be signed.
- For the virtual remote interview, the consent form will be sent via JISC.
- Face-to-face interviews will be audio-recorded and subsequently transcribed verbatim, thereby creating the primary qualitative dataset.
- Field notes will be taken during and immediately after interviews to capture contextual observations and reflections.

Secondary data will be collected through the gathering of relevant organisational and publicly available documents, including sustainability policies, procurement guidelines, supplier codes of

conduct, carbon reporting materials, and regulatory or industry guidance documents. These materials will be used to contextualise and triangulate the interview data.

Documentation and Metadata

What documentation and metadata will accompany the data?

All data generated during this research will be supported by appropriate documentation and metadata to ensure the data are understandable, interpretable, and reusable, in accordance with the University of Plymouth Research Data Management Policy and good research practice.

For primary qualitative interview data, the following documentation will be maintained:

- Participant Information Sheets and Consent Forms, detailing the purpose of the research, data collection procedures, data storage, retention, and participants' rights, including withdrawal.
- An interview schedule and protocol, documenting the semi-structured questions and prompts used consistently across interviews.
- Anonymised participant identifiers (e.g. SME1, SME2) to enable internal referencing while protecting confidentiality.
- An interview log, recording the date, duration, mode of interview (online or face-to-face), and participant role.

For interview transcripts and qualitative datasets, accompanying metadata will include:

- Date and location (or platform) of data collection.
- Recording and transcription methods used (e.g. verbatim transcription).
- Any transcription conventions applied.
- Version control information for transcripts and coded files.

For secondary and documentary data, metadata will include:

- Source of the document (organisation, policy body, or public repository).
- Document type (e.g. sustainability policy, procurement guideline, carbon report).
- Date of publication or issue.
- Relevance to the research objectives.

For data analysis, additional documentation will be created to support transparency and reproducibility:

- A coding framework, detailing themes and sub-themes developed during analysis.
- Analytical and reflexive memos, explaining interpretive decisions and theoretical reasoning.
- An audit trail, documenting changes made to codes and themes throughout the analytical process.

All files will be accompanied by a README file describing file naming conventions, folder structure, abbreviations, and relationships between datasets. Metadata will be recorded clearly and consistently to ensure that the data remains intelligible beyond the life of the project.

Ethics and Legal Compliance

How will you manage any ethical issues?

Ethical issues will be managed in accordance with the **University of Plymouth Research Ethics Policy** and principles of informed consent, confidentiality, and participant welfare.

Before data collection, all participants will receive a **Participant Information Sheet** explaining the purpose of the study, what participation involves, how data will be used, stored, and retained, and their right to withdraw without penalty. **Written informed consent** will be obtained before interviews commence.

Participant confidentiality will be protected through **anonymisation**, with identifiers replaced by pseudonyms (e.g. SME1). No personally identifiable or commercially sensitive information will be disclosed in publications. All digital data will be stored on **password-protected, encrypted university-approved systems**, accessible only to the researcher and supervisory team.

Potential risks, such as discomfort when discussing organisational pressures or sustainability challenges, will be minimised by allowing participants to **decline to answer questions or stop the interview at any time**. No vulnerable groups are targeted, and no deception will be used.

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

Managing copyright and Intellectual Property Rights (IPR) is essential to ensure that the research respects the rights of all contributors and sources. Here are the steps to be taken:

1. Identify and Attribute Sources:

All sources of data, literature, and other intellectual content will be properly cited and attributed according to academic standards (e.g., Harvard referencing style). Any use of third-party materials (such as images, figures, or proprietary data) will be clearly

credited to the original creators.

2. Obtain Permissions:

Permissions will be sought for the use of any copyrighted materials that are not covered by fair use or academic exemptions. Written consent will be obtained from stakeholders and data providers when their proprietary information or data is used.

3. Original Work:

Ensure that all work produced is original and does not infringe on the IPR of others. Any collaboration or co-authorship will be clearly defined, and contributions will be appropriately acknowledged.

4. Data Ownership:

Clarify the ownership of data collected during the research. Typically, the researcher or the institution conducting the research will own the data.

Participants will be informed about how their data will be used, stored, and shared, and they will provide consent for these uses.

5. Institutional Policies:

Adhere to the University of Plymouth’s policies on intellectual property and copyright. Any research outputs (e.g., publications, reports) will comply with the university’s guidelines on IPR.

6. License Data:

When sharing data, appropriate licenses (such as Creative Commons licenses) will be used to specify how the data can be used by others. Ensure that the necessary licensing agreements accompany data shared with external parties.

7. Publication and Dissemination:

Before publishing or disseminating research findings, ensure that no confidential or proprietary information is disclosed without proper authorisation. Co-authors and contributors will be acknowledged appropriately in all publications.

8. Plagiarism Prevention:

Use plagiarism detection tools to ensure that all content is original and properly referenced. Maintain a high standard of academic integrity by avoiding any form of plagiarism or uncredited use of others' work.

Storage and Backup

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

To ensure the data is securely stored and backed up during the research, the following measures will be implemented:

1. Data Storage Locations:

Primary Storage: Data will be primarily stored on the University of Plymouth's secure servers. These servers offer robust security measures, including firewalls, encryption, and access controls.

Secondary Storage: A secondary backup will be maintained on an external hard drive or cloud storage service approved by the university, such as Google Drive or Microsoft OneDrive, to ensure redundancy.

2. Data Backup:

Regular Backups: Data will be backed up regularly, with automated daily backups scheduled to minimise the risk of data loss.

Version Control: A version control system will be implemented to keep track of changes and ensure that previous versions of data files can be restored if needed.

3. Security Measures:

Encryption: All sensitive data will be encrypted both in transit and at rest to protect it from unauthorized access.

Access Control: Access to data will be restricted to authorised personnel only. This will be managed through secure login credentials and multi-factor authentication (MFA).

Data Anonymisation: Any personal or sensitive information will be anonymised or pseudonymized to protect participant identities and comply with GDPR requirements.

4. Data Management Plan (DMP):

A comprehensive Data Management Plan will be developed and adhered to, detailing procedures for data handling, storage, and backup throughout the research project.

The DMP will include protocols for secure data transfer, storage locations, backup schedules, and access controls.

5. Regular Audits:

Regular audits will be conducted to ensure compliance with the data management plan and identify any potential security vulnerabilities or breaches.

6. Emergency Procedures:

An emergency recovery plan will be in place to quickly restore data from backups in the event of hardware failure, data corruption, or other unforeseen events.

This plan will include clear steps for data restoration and communication protocols to inform relevant stakeholders.

7. Documentation:

Detailed documentation of data storage locations, backup procedures, encryption methods, and access controls will be maintained.

Documentation will be regularly updated to reflect any changes in data management practices.

How will you manage access and security?

To manage access and security for the research data, the following basic measures will be implemented:

1. Access Control:

User Authentication: Only authorised individuals will have access to the data, using secure login credentials.

Role-Based Access: Access will be granted based on roles, ensuring individuals only access the data necessary for their tasks.

2. Data Encryption:

In Transit: Data transferred over networks will be encrypted to protect it from interception. At Rest: Stored data will be encrypted to prevent unauthorised access.

3. Physical Security:

Secure Storage: Servers and storage devices will be kept in locked, access-controlled rooms.

4. Data Anonymisation:

Anonymisation: Personal or sensitive information will be anonymised to protect the participant's identities.

Pseudonymization: Where anonymisation is not possible, pseudonymization techniques will be used.

5. Monitoring and Audits:

Access Logs: Logs of data access will be maintained and reviewed regularly to detect unauthorized access.

Security Audits: Periodic security checks will be conducted to identify and fix vulnerabilities.

6. Data Management Policies:

Policy Documentation: Data management policies will be documented and followed by all personnel.

Training: All personnel will be trained on data security practices.

7. Incident Response:

Plan: An incident response plan will be in place to handle data breaches or security incidents promptly.

8. Regulatory Compliance:

GDPR Compliance: Compliance with GDPR and other data protection regulations will be ensured, including obtaining participants' informed consent.

Selection and Preservation

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

The following data from the research are of long-term value and should be retained, shared, and/or preserved:

1. Interview Transcripts:

Retention and Preservation: These transcripts provide detailed insights and qualitative data valuable for future studies and analysis.

Sharing: Anonymised versions can be shared with other researchers to contribute to the broader body of knowledge in Operations and Supply Chain Management (OSCM).

2. Semi-structured Interview Guide:

Retention and Preservation: interview responses offer qualitative data that can support empirical studies and trend analysis.

Sharing: Anonymised and gathered data can be shared with academic and industry researchers to facilitate further research.

3. Case Study Findings:

Retention and Preservation: The detailed multiple-case study of Plymouth Manufacturer’s Group (SMEs) OSCM practices is a valuable resource for future research and reference.

Sharing: Findings can be published in academic journals and shared at conferences to disseminate knowledge.

4. Data Analysis Results:

Retention and Preservation: Analysis results, including thematic analyses and statistical summaries, provide valuable insights that can inform future research and practice.

Sharing: Summary data and key findings can be included in research publications and shared with stakeholders.

5. Documentation and Metadata:

Retention and Preservation: Detailed documentation and metadata about the research process, methodologies, and data collection techniques ensure the reproducibility and reliability of the research.

Sharing: Documentation can be shared with other researchers to enhance transparency and facilitate further studies.

6. Research Reports and Publications:

Retention and Preservation: Final research reports and published papers represent the culmination of the research efforts and are crucial for academic records.

Sharing: These documents should be widely shared through academic publications, university repositories, and research networks.

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

The long-term preservation plan for the dataset involves several key steps to ensure the data remains accessible, secure, and usable for future research. Here are the main components of the plan:

1. Archiving in a Secure Repository:

Institutional Repository: The dataset will be archived in the University of Plymouth's institutional repository, which ensures secure, long-term storage and management.

External Repositories: Additionally, copies of the dataset can be deposited in external, trusted data repositories like Zenodo or Figshare, which are designed for long-term data preservation and access.

2. Regular Backups:

Automated Backups: Implement regular automated backups to protect against data loss. This includes maintaining copies on secure servers and external storage devices.

Geographically Distributed Backups: Ensure that backups are stored in multiple geographical locations to mitigate the risk of data loss due to local disasters.

3. Data Format and Documentation:

Non-Proprietary Formats: Store data in non-proprietary, widely-used formats such as CSV, TXT, and PDF to ensure long-term accessibility regardless of future software changes.

Comprehensive Documentation: Maintain comprehensive documentation and metadata, including data dictionaries, methodology descriptions, and analysis procedures, to facilitate future understanding and reuse of the data.

4. Access and Usage Policies:

Controlled Access: Implement controlled access measures to ensure that only authorised users can

access sensitive data. This includes password protection and user authentication.

Data Sharing Agreements: Establish data sharing agreements to govern the terms under which data can be shared with external researchers, ensuring compliance with ethical and legal standards.

5. Regular Review and Maintenance:

Periodic Review: Conduct periodic reviews of the dataset to ensure its continued relevance and integrity. This includes checking for data corruption and updating documentation as needed.

Maintenance Plan: Develop a maintenance plan that includes scheduled updates, data integrity checks, and migration to new storage technologies as they become available.

6. Data Access and Citation:

Persistent Identifiers: Assign persistent identifiers (such as DOIs) to the dataset to facilitate citation and long-term access.

Open Access: Where appropriate and ethical, make the dataset openly accessible to promote wider dissemination and use in future research.

Data Sharing

How will you share the data?

To ensure the data is effectively shared while maintaining security and accessibility, the following plan will be implemented:

1. Publishing in Data Repositories:

Institutional Repository: The dataset will be deposited in the University of Plymouth’s institutional repository (PEARL), which ensures long-term access and management.

Public Data Repositories: The dataset will also be shared in trusted public repositories such as Zenodo or Figshare, which provide persistent identifiers (DOIs) and ensure broad accessibility.

2. Documentation and Metadata:

Comprehensive Metadata: Include detailed metadata and documentation to help other researchers understand the dataset, including descriptions of data collection methods, variables, and any processing steps.

Data Dictionaries: Provide data dictionaries that explain the variables and coding schemes used in the dataset.

3. Access Control:

Open Access: For non-sensitive data, make the dataset openly accessible to the public under a Creative Commons license to encourage reuse and citation.

Restricted Access: For sensitive data, implement controlled access protocols. This may involve requiring users to register, agree to data use agreements, or obtain permission before accessing the data.

4. Data Sharing Agreements:

Formal Agreements: For data that cannot be fully open due to ethical or legal reasons, establish data sharing agreements that specify the terms of use, including restrictions on redistribution and obligations to maintain confidentiality.

5. Publication of Findings:

Journal Articles: Publish research findings in academic journals and include links to the dataset within these publications, allowing readers to access the data directly.

Conference Presentations: Present findings at conferences and include references to where the data can be accessed.

6. Collaborations and Networks:

Research Networks: Share the dataset with relevant research networks and professional groups to facilitate collaboration and further research.

Workshops and Seminars: Organise workshops and seminars to share insights from the data and encourage its use by other researchers.

7. Online Platforms:

Project Website: Create a project website or a dedicated page on the university's website to host the dataset and related resources. This site can also provide updates on ongoing research using the data.

Social Media and Academic Networks: Promote the availability of the dataset through social media platforms and academic networks such as ResearchGate and LinkedIn to reach a wider audience.

Are any restrictions on data sharing required?

Yes, several restrictions on data sharing need to be considered to ensure ethical and legal compliance:

1. Confidentiality and Privacy:

Personal Data Protection: If the data includes personal information, ensure that any shared data complies with data protection laws such as GDPR. This may involve anonymising data to protect the identities of participants.

Sensitive Information: For data involving sensitive topics, apply additional restrictions to ensure participant privacy and confidentiality.

2. Ethical Considerations:

Informed Consent: Ensure that all participants have provided informed consent for their data to be shared. This consent should include information about how the data will be shared and who will have access to it.

Ethical Approval: Any data sharing must align with the ethical approval obtained for the research. This includes adhering to any conditions or limitations specified by the ethics committee.

3. Intellectual Property Rights (IPR):

Copyright and IPR Compliance: Ensure that sharing the data does not infringe on copyright or intellectual property rights. This includes respecting third-party data sources and their sharing restrictions.

4. Commercial Sensitivity:

Proprietary Information: If the data contains proprietary or commercially sensitive information, restrict access to prevent misuse or unauthorised commercial exploitation.

Non-Disclosure Agreements (NDAs): For particularly sensitive data, consider using NDAs to legally bind users to confidentiality terms.

5. Controlled Access:

Restricted Access: Implement controlled access measures for data that cannot be fully open. This can include requiring registration, data use agreements, or specific permissions to access the data.

Tiered Access Levels: Differentiate between datasets that can be fully open and those that require restricted access based on their sensitivity.

6. Usage Restrictions:

Data Use Agreements: Require users to sign data use agreements that specify acceptable uses of the data and prohibit activities such as re-identifying individuals or using the data for non-research purposes.

Attribution Requirements: Ensure that users properly attribute the data source in any publications or presentations.

Responsibilities and Resources

Who will be responsible for data management?

The responsibility for data management will be assigned to several key roles to ensure comprehensive and effective handling throughout the research project:

1. Principal Investigator (PI):

The PI will oversee the overall data management plan, ensuring all protocols and guidelines are followed. The PI will also coordinate with team members to ensure data integrity, security, and compliance with ethical standards.

2. Data Manager:

A dedicated Data Manager will handle the day-to-day tasks of data management, including data collection, storage, and backup processes. This person will also be responsible for maintaining documentation and metadata.

3. IT Support Staff:

IT support staff will provide the necessary technical infrastructure for secure data storage and backup. They will also ensure that all data management systems are functioning correctly and that access controls are properly implemented.

4**. Ethics and Compliance Officer:**

An Ethics and Compliance Officer will be responsible for ensuring that all data management activities comply with ethical guidelines and legal requirements. This includes verifying that informed consent is obtained and that data sharing restrictions are adhered to.

By delineating these responsibilities, the research project will maintain high standards of data management, ensuring that data is handled ethically, securely, and effectively throughout its lifecycle

What resources will you require to deliver your plan?

To implement the data management plan effectively, the principal researcher will need access to suitable data management software or platforms, adequate storage infrastructure, IT support for maintenance and troubleshooting, and potentially budgetary allocations for any required software licenses or additional storage capacity.