Digital Support Partnership Research Project Data Management Plan

0. Proposal name

Digital Support Partnership Research Project

1. Description of the data

1.1 Type of study

The Digital Support Partnership is a 14 month strategic project which brings together expertise from across the university to ensure student engagement with learning and teaching over the academic year 2020-21, while also maintaining a focus on staff and student wellbeing during this time. The research component of this project seeks to evaluate the effectiveness of this approach for staff and students, interrogate the resources and materials produced and investigate student experience of online learning and teaching during this academic year.

1.2 Types of data

Both quantitative and qualitative data will be used in the research. Data will be gathered from:

- *university student surveys (led by the student survey team)
- student focus groups
- staff surveys,
- staff focus groups
- staff support materials
- staff reflective accounts
- staff interactions with the Moodle Community
- **usage statistics for university learning technologies from IS

The raw data will take the form of digital survey answers, digital video and audio from online focus groups (deleted after transcription) and digital transcriptions of focus groups, digital text contributions to discussion forums and anonymised tracking and participation statistics from Moodle.

*Please note, data collected from the university student surveys will anonymised by the student survey team before being passed to the research team.

**Please note, usage statastics will not contain any personal identifiers and will be collected by IS and passed to the research team.

1.3 Format and scale of the data

Video and audio files: MP4s focus group meeting recordings, extracted as audio MP3 (Webex)

Transcript files: MS Word

Survey and IS reports results: Excel

Staff support materials: Word, JPG/PNG, MP4

Analysis files: Nvivo 12 imported from Word

Numbers of records can only be estimated at this point, with student responses up to 1000, with currently two planned sweeps in Tr1. An estimate of staff records would be 250.

2. Data collection / generation

2.1 Methodologies for data collection / generation

Student digital survey data will be gathered by the student surveys team (not part of this project) who will anonymise it before passing it to the research team, in the format of Excel files for storage on the X Drive.

The online student focus groups will be led by Kirsty McKay and Student Futures members. Kirsty McKay will record the meetings on Webex to her university Webex cloud account will be the sole person with access to that recording. She will use Webex close captioning to generate a transcription, which she will then edit for accuracy and anonymise the data. After transcription she will delete the Webex recording and all associated files with the meeting including attendance records. The transcriptions will be in the form of Word documents which will be stored on the X Drive.

The online staff survey will be administered by the research team and data will be gathered via the NOVI survey tool.

The online staff focus groups will be led by a member of the research team, who will record the meetings on Webex to their university Webex cloud account will be the sole person with access to that recording. They will use Webex close captioning to generate a transcription, which they will then edit for accuracy and anonymise the data. After transcription they will delete the Webex recording and all associated files with the meeting including attendance records. The transcriptions will be in the form of Word documents which will be stored on the X Drive.

Staff support materials exist on the DLTE intranet site and are publicly available and on the project Moodle community which is accessible by all staff members. Data will be gathered from these sites by the research team and will take the form of text (in documents), images and some videos (MP4). A member of the research team will remove any personal data and metadata in these files before analysis.

Staff reflective accounts will be in the form of Word documents and will be anonymised by the authors. A member of the research will copy the text into new files so as to remove any identifying metadata and delete the original files. Text collected from the Moodle Community site by the research team will be anonymised by the research team before being saved in Word documents. Reports from IS about Moodle and other learning technologies will be generated by IS, who will remove any personal identifiers such as IP addresses before passing the reports to the research team.

All files will be stored on the X Drive with password protected access for the research team only.

2.2 Data quality and standards

The research team will check for accuracy of data before and after any data processing.

3. Data management, documentation and curation

3.1 Managing, storing and curating data.

Research data will be stored on the University's X:drive. University-managed data storage is resilient, with multiple copies stored in more than one physical location and protection against corruption. Daily backups are kept for 14 days and monthly backups for an additional year.

3.2 Metadata standards and data documentation

All research data will be organized as per the Universities metadata standards http://staff.napier.ac.uk/services/research-innovation-office/research-data/Pages/Organising.aspx

3.3 Data preservation strategy and standards

The Edinburgh Napier Data Management Policy states requires research data to be retained after project completion if they substantiate research findings, are of potential long-term value or support a patent for at least 10 years. Long term storage is provided through the University data repository.

4. Data security and confidentiality of potentially disclosive information

All respondents will be asked for explicit consent and provided with the research information sheet.

The **online student focus** groups will be led by Kirsty McKay and Student Futures members. Kirsty McKay will record the meetings on Webex to her university Webex cloud account and will be the sole person with access to that recording and the meeting meta data. She will use Webex close captioning to generate a transcription, which she will then edit for accuracy and anonymise. After transcription she will delete the Webex recording and all meta data and associated files with the meeting including attendance records.

The **online staff survey** will be administered by the research team and data will be gathered via the NOVI survey tool. The survey will not ask for any personal data and one member of the research team will remove any meta data such as IP addresses before saving the data to the X Drive.

The **online staff focus** groups will be led by members of the research team. One researcher will record the meetings on Webex to their university Webex cloud account and will be the sole person with access to that recording and the meeting meta data. They will use Webex close captioning to generate a transcription, which they will then edit for accuracy and anonymise. After transcription they will delete the Webex recording and all meta data and associated files with the meeting including attendance records.

The **staff support materials** were generated by the project and do not include any personal data.

Staff anonymous reflective accounts will be submitted via MS Forms which have been set up not to record any personal identifying data or metadata. The Excel file which holds the responses will be checked by one member of the research team to anonymise any responses which include identifying data, after which the original Excel fill will be deleted.

Text collected from the **Moodle Community** site by the research team will be anonymised by the research team before being saved in Word documents.

Learning technologies usage statistics from IS about will be generated by IS and will not contain any personal data.

4.1 Formal information/data security standards

Data generated by the **student surveys** are collected by the student survey team and will be completely anonymised before being passed to the research team. The data will include the following special category data (but individuals will not be identifiable):

- racial or ethnic origin;

- religious beliefs;
- physical or mental health;
- sexual orientation;

All names and contact information will be removed from the data and replaced with a numeric identifier that cannot be linked to any individual. All files will be held on a secure server.

4.2 Main risks to data security

All data will be checked for anonymity and/or deidentification by one member of the research team, before being passed to the researchers for analysis. The main risks to participants would be before this point. To ensure there is no risk to a student being taught by a member of the research team, the programmes where the researchers are lecturers will be eliminated from the research data. Personal data contained in the surveys will be anonymised before being passed to the research team. A space on the X Drive has been requested and all raw and processed data used in the research will be solely stored there. All participants will be provided with a research information sheet and a consent form.

MRC guidance on the Confidentiality and data security is provided (please see page 24 of the PDF file generated by selecting the above or adjacent link).

5. Data sharing and access

Identify any data repository (-ies) that are, or will be, entrusted with storing, curating and/or sharing data from your study, where they exist for particular disciplinary domains or data types. Information on repositories is available here.

5.1 Suitability for sharing

Data generated by the project (identified above) will be made open once appropriate changes have been made to honour assurances of confidentiality and anonymity.

5.2 Discovery by potential users of the research data

Datasets will be allocated a DOI and stored on our open access Research Repository in accordance with the University research data deposit process. The DOI and the datasets will be made available to the UK Data Service ReShare repository within three months of the end of the grant.

5.3 Governance of access

The research team in consultation with the research gatekeeper will govern access to the data.

5.4 The study team's exclusive use of the data

This is not funded research, so exclusive use of data does not apply.

5.5 Restrictions or delays to sharing, with planned actions to limit such restrictions

There are no restrictions or delays.

5.6 Regulation of responsibilities of users

External users are (will be) bound by data sharing agreements, setting out their main responsibilities (please see page 13 section 7, titled Data-sharing agreements of the PDF file generated by selecting either of two links above).

6. Responsibilities

The first point of contact for all queries in relation to this data is the PI. Who will also have overall responsibility for the production and maintenance of metadata. Preparation and upload of the data will be carried out by the team with the support of the University's Information Services staff.

7. Relevant institutional, departmental or study policies on data sharing and data security

Please complete, where such policies are (i) relevant to your study, and (ii) are in the public domain, e.g. accessible through the internet.

Add any others that are relevant

Policy	**URL or Reference**
Data Management Policy & Procedures	https://staff.napier.ac.uk/services/research-innovation-office/Documents/Research%20Data%20Management%20Policy.pdf https://staff.napier.ac.uk/services/research-innovation-office/research-data/
Data Security Policy	https://staff.napier.ac.uk/services/research-innovation-office/research-data/Pages/Storing-Data.aspx https://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx
Data Sharing Policy	*https://staff.napier.ac.uk/services/research-innovation-office/research-data/Pages/Sharing-and-Re-Use.aspx* https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/DataSharing.aspx
Institutional Information Policy	*https://staff.napier.ac.uk/services/secretary/governance/Pages/Governance.aspx* https://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx
Other:	

8. Author of this Data Management Plan (Name) and, if different to that of the Principal Investigator, their **telephone & email contact details**

Louise Drumm

l.drumm@napier.ac.uk