

|  |  |
| --- | --- |
|  | |
| Research: Data Privacy Impact Assessment (DPIA) |
| Jayne Woodside |
| The CANTEEN Study: Free School Meals, Diet Quality and Food Insecurity in Secondary School Pupils: a Mixed Methods Study |
| If you have any queries, please contact the Information Compliance Unit (ICU) info.compliance@qub.ac.uk | |

**Introduction:**

This Data Privacy Impact Assessment (DPIA) has been created specifically for academic research. It is designed to help you think about the data you will be collecting, processing, storing and transferring as part of your research/study. You will be asked to list the types of data and data fields to be collected. As well as details on the storage and transfer. It will help focus your thinking about the personal and sensitive data to be collected and whether the data can be ‘minimised’ to help reduce risk. Guidance notes have been produced to assist with its completion.

This document is a living document, which will be updated as and when required throughout the duration of the research project lifecycle.

The Information Compliance Unit (ICU) and the Data Protection Officer (DPO) will provide advice and guidance based on the information provided within the assessment, which can be found at the end of the assessment. This will discuss any recommendations on how to further safeguard the personal/sensitive data and whether there are any actions required to comply with the legislation (Data Protection Act 2018 and the General Data Protection Regulation).

**Project Summary:**

Please briefly detail what the project is about and what it plans to achieve:

Food insecurity is common in children and is consistently linked with poor health outcomes. Free School Meal provision is a government-implemented means-tested strategy intended to improve food insecurity and nutrition and reduce dietary inequalities. FSM eligibility is increasing, with concerns that food insecure children are not always eligible for FSM based on current criteria. FSM uptake is also variable, with 20% of eligible secondary pupils not taking FSM. Little research has examined the impact of the current means-tested FSM policy on food intake, diet quality and food insecurity, particularly at secondary level. Evidence of effectiveness of the current FSM policy is essential to support the status quo, but also to inform recently proposed changes. In addition, little is known about what influences whether FSM-eligible children take these up. This research aims to conduct a mixed methods study (observational study and case study) toevaluate the effectiveness and cost-effectiveness of the current means-tested FSM policy in UK secondary schools on diet and food insecurity outcomes, understand what factors are associated with uptake, and test the potential impact of the proposed policy change.

Research questions

1) What is the effectiveness and cost-effectiveness of the FSM policy in UK secondary schools on FV intake and overall diet quality?

2) What is the effectiveness and cost-effectiveness of the FSM policy on food insecurity, attendance and educational attainment?

3) What would be the effect of FSM policy changes on FV intake, diet quality and food insecurity?

4) What school factors are associated with differences in FSM uptake?

Objectives to address the research questions:

1. Undertake an observational study (n=32 secondary schools; n=1440 pupils and one of their parents/ guardians at two sites –Midlands: n=16 schools, years 7 and 10 and Northern Ireland: n=16 schools, years 8 and 11 - pupils aged 11-12 years and 14-15 years) to investigate the means-tested FSM policy, utilising the variation in FSM uptake and collecting school-level factors and parent- and pupil level outcomes (RQ1-3)

2. Conduct multi-level modelling of pupil outcomes on FSM uptake at the school-level to evaluate the association between FSM uptake levels and FV intake, overall diet quality, and food insecurity in all pupils, irrespective of FSM status (RQ1,2), also exploring aggregated attendance and educational attainment data.

3. Conduct multi-level modelling to compare FSM eligible pupils who take FSM and FSM eligible pupils who do not take FSM and assess the effect of FSM uptake on FV intake, diet quality, and food insecurity (RQ1,2).

4. Conduct economic analysis of FSM uptake, using a cost-utility approach (RQ1,2).

5. Model policy change impacts of extending FSM eligibility and increasing uptake on FV intake, overall diet quality and food insecurity (RQ1,2,3).

6. Conduct a case study to assess barriers and facilitators and characterise schools with different levels of FSM uptake (RQ4) in a subset of the recruited schools. Focus groups (n=6-8) will be conducted with pupils (x3 groups of 8 pupils per school) and interviews will be conducted with parents (n=8 per school) and key school stakeholders (e.g. catering and finance manager and school principal) (n=4 per school).

7. Conduct workshops to gain stakeholder views on study findings and guide future intervention (dissemination).

**1. Categories of personal/sensitive data to be collected:**

Contact details:

Including names, address, phone number etc.

Physical and health data:

Including physical appearance, health related data, weight, height etc.

Tracking data:

Including IP addresses, GPS or detailed location data.

Demographic data:

Including job, income, age, education, race, religion, marital status etc.

Sexual data:

Including gender identity, preferences, history etc.

Knowledge and Preference data:

Including thoughts, feelings, opinions, preferences etc.

Digital recordings:

Any data you are collecting which involves video, voice recordings or images.

Children’s data:

Please indicate here if any children’s data will be collected as part of the study.

Criminal data:

Please indicate here if you will be collecting or recording any data related to criminal convictions (alleged, serving or spent).

Trade Union Membership:

Please indicate here if you will be collecting details on trade union membership.

**2. Data Fields to be collected**

For each data type selected above, please now detail the data fields you intend to collect. However, a relatively low level of granularity is required at this point of the assessment. For example, if you require details of a name, then add ‘Full Name’. Do not add ‘First Name’, ‘Middle Name(s)’, ‘Family Name’ or for address ‘First line’, ‘Second line’ etc. Also, when detailing the data items to be collected, they can be grouped into ‘opinions on [insert study focus]’. For example, a study which requires participants to give their thoughts on a service could list ‘Opinions on rehabilitation service patient outcomes’ and not a list of each question within the survey asking for an opinion.

Contact Details:

* Pupils: Full name
* Parent/ guardians and school staff/ stakeholders: Full name, email address

Physical and Health:

* Pupils: Dietary intake, physical activity level, quality of life, if registered as having special educational needs

Tracking: None collected

Demographic:

* Pupils: Home postcode, school year group, date of birth, sex, ethnicity , food insecurity, Free School Meal eligibility, whether English is an additional language, educational attainment
* Parent/ guardian: Sex, age group, ethnicity, food insecurity, child’s Free School Meal eligibility
* School staff/ stakeholders: Sex, age group

Sexual: None collected

Knowledge and Preference:

* Pupils: Views on their school food environment, school food provision and school food education
* Parent/ guardian and school staff/ stakeholders: views and experiences of Free School Meals and views on the school food environment, school food provision and school food education

Digital Recordings:

* Pupils Focus groups and parent/ guardian and school staff/ stakeholder interviews to explore views on factors that may be associated with Free School Meal uptake (Including barriers and facilitators to Free School Meal uptake, school food systems, Free School Meal system, school meal provision in general and the school food environment)

**3. Data Flows:**

We should now detail the flow of data from the point of collection, through to processing, storage and sharing/transfer.

It is important to consider all possible eventualities for potential sharing of data, as it is imperative that we notify the data subjects, prior to processing and transfer, as to who their data will be shared with and why.

Method(s) of data collection: In this section, please detail the method and medium of data collection (face-to-face interviews, surveys etc.)

Cross-sectional study

* Participants (pupils, parents/ guardians and school staff/ stakeholders) will complete questionnaires using Qualtrics survey software
* Pupils will complete an online dietary survey (24 hour recall) using the INTAKE 24 online dietary recall system
* Schools will provide information on pupils that take part (their educational attainment, whether they are eligible to receive Free School Meals, whether English is an additional language for them, and if they are registered as having any special educational needs)
* Aggregated attendance data, educational attainment data (GSCE data) and school meal data including uptake will be provided by schools
* Direct observation of school eating environments by a researcher (using school food environment observation tool)
* Analysis of key school documents and policies (including school promotion of Free School Meals, Free School Meal eligibility, registration processes for Free School Meals, school food policies, other relevant school policies and relevant inspection reports)

Case study

* Face-to-face focus groups with pupils at school
* Face-to-face or online interviews with parents/ guardians, school staff and stakeholders

Post-study dissemination workshops

* Online workshops with school food stakeholders including the government, school catering, parents and pupils

Data Storage: Please detail where the data, once collected as specified above, will be stored during processing and analysis.

During the study, hard copy data collected in England will be stored in a locked filing cabinet in a locked office in a secure building at the Institute of Applied Health Research, University of Birmingham. Only members of the research team at the University of Birmingham will have access to the cabinet. Hard copy data collected in Northern Ireland will be stored in a locked filing cabinet in a locked office (the Chief Investigators office, room 01.028, Institute of Clinical Sciences A) in a secure building at the Centre for Public Health, Queen’s University Belfast. Members of the research team at Queen’s University Belfast will have access to the cabinet.

All study data in electronic form will be downloaded from Qualtrics survey software or INTAKE 24 online dietary recall system and stored confidentially (anonymised using ID numbers) and held securely on University network servers. Access will be password protected and restricted to researchers with designated responsibility for the conduct of the study or encrypted machines protected by passwords. Identifiable information (e.g. consent forms) will be stored separately from other data (e.g. questionnaires). When the full dataset has been downloaded from Qualtrics and INTAKE 24, data will be permanently removed from these softwares. Collected data will be stored in this way by Queen’s University Belfast and the University of Birmingham during the study period.

Personal data and Sensitive Personal data provided by schools about pupils taking part in the study (educational attainment, whether they are eligible to receive Free School Meals, whether English is an additional language for them, and if they are registered as having any special educational needs) will be be provided to the research team via email in a password protected excel file. Alternatively, schools will provide this information to the research team face-to-face as a paper copy that will be temporarily stored in a locked filing cabinet in a locked office in a secure building at the Centre for Public Health, Queen’s University Belfast or the Institute of Applied Health Research, University of Birmingham. Paper copies of this information will be entered onto excel by the research team and then the paper copy destroyed. All personal data and Sensitive Personal data will be pseudonymised post collection and stored in a separate database to other study data.

Study collaborators at Newcastle University will directly access dietary intake data as it will be collected through the online Intake24 tool, which is owned by Newcastle University. However, they will not have any access to corresponding personal identifiable data from participants (participants will use pre-generated usernames to log-in to this software).

Data Transfer: Please detail here below how data will be transferred from point of collection to storage and any subsequent transfers that are required. **Also, please indicate here if any data will be transferred outside of the European Economic Area (EEA)**

Study documentation will be kept for 10 years after the end of the study/ publication of data in-line with requirements from the sponsor and will be held securely in the custody of the CI. At the end of this period the CI will review the data to determine whether or not there is a need to retain any of the data beyond this time point. Data that are no longer required will be securely destroyed (shredded and disposed in confidential waste) in line with QUB policy.

Personal data (e.g. name or any data from which a participant might be identified) will not be kept for longer than is required for the purpose for which it has been acquired. At the end of the study, each site will send original source documentation (hard copy or electronic) along with consent forms and contact details for individuals who have provided consent to be contacted about future related studies to QUB for archive. Sites will be responsible for archiving general site files accumulated during the day-to-day operation of the study. Only members of the research team will have access to personal information.

Participants who consent to take part in study interviews will provide information, which will be recorded using a digital recorder. Audio files will be downloaded to password-protected systems, named according to the participant’s unique study ID and transferred securely via secure encrypted file transfer to a QUB approved transcription service. The transcription service provider will be required to sign a confidentiality agreement. Audio files will be transcribed verbatim and transferred back to QUB via the secure Dropoff facility. They will be stored on password protected computer systems as for all other electronic data. When transcripts are received, they will be checked for accuracy against the audio recordings and any potentially identifiable information with the transcript such as names will be removed. Audio recordings will be destroyed when it has been satisfied that the transcript is an accurate written record of the interview. Data from qualitative interviews will be anonymised by removing any information which could potentially identify the participant. Only interview transcribers who are approved by the sites and meet confidential data handling requirements will be used. Each participant will have a unique participant study ID. The interview recordings, transcriptions and NVivo database will be password protected, encrypted, and stored securely as for other files. When transcripts have been prepared and checked for accuracy, the recordings will be deleted.

**4. Data Minimisation:**

This is one of the seven principles of GDPR and forms an important part of the DPIA process. One of the main differences between this GDPR principle and the former DPA 1998 (adequacy) principle, is the need to demonstrated appropriate data minimisation practices. This will be done via the DPIA.

What to consider:

* Identify the minimum amount of data required to fulfil your purpose.
* Ask yourself ‘why do I need this data?’
* Periodically review processing to check that the personal data you hold is still relevant and adequate for your purposes.
* Consider what the data is needed for and whether it is all or part of that is required.

An example of data minimisation is as follows:

Date of birth (DOB) is required to be captured to calculate the age of the participant. As DOB can be used in conjunction with other data to identify an individual (or used to build a profile of a data subject), ask the question as to whether you require the specific DOB or if your simply require their age. This is still personal data but we have reduced the risk associated with holding/processing because in longer takes to the form of a DOB.

Pupil full name and pupil date of birth will be collected from both pupils and parents for the purposes of matching child and parent data. Full name and email address will be collected from parents and school staff/ stakeholders to enable provision of study vouchers. These data will be stored in a separate database to other study data and will only be accessible to the research team. Personal data will only be stored until pupil and parent data has been matched and vouchers distributed at which point it will be removed. Participants will be informed of this in participant information sheets. The reason for collecting these matching variables is because of a previous similar study carried out by the University of Birmingham, who are a site lead here, where data could not be matched because of errors in ID entry. The following information will also be collected from parents and pupils: Home postcode be collected for calculation of Index of Multiple Deprivation to address study aims; and school year group and ethnicity to capture the population demographics.

Schools will provide the following information on pupil’s taking part in the study: educational attainment, whether they are eligible to receive Free School Meals, whether English is an additional language for them, and if they are registered as having any special educational needs. This information is being collected for the purpose of being able to understand more about the relationship between different pupil characteristics and uptake of Free School Meals. All personal data and Sensitive Personal data will be pseudonymised post collection and stored in a separate database to other study data.

**5. Processes of Pseudonymisation or Anonymisation:**

If you are protecting the personal or sensitive data through a process of pseudonymisation or anonymisation, please detail below how this will be achieved. Please note, if you remove a name or another identifier, replace it with a unique identifier but retain other linked data, this is pseudonymised.

Personal data that is not anonymised will be collected for the purposes of management of the research to match up data provided by children to data provided by their parent/ guardian and also for provision of study vouchers and will not be stored once these processes are completed. All other study data will be anonymised with unique ID numbers so that individuals cannot be identified. Participants will not be identifiable from any presentation or publication from the study. Direct focus group and interview quotations collected from participants during the study may be used in publications, but will be pseudonymised so as not to allow identification of individuals.

**6. Data Sharing:**

If, in section 3, you have indicated that there are to be other recipients of the data, please detail below all these recipients, what data and format they will receive and for what purpose:

|  |  |  |
| --- | --- | --- |
| Recipient (Name/Company): | Data/format: | Purpose: |
| Queen’s University Belfast research personnel | All data collected during study | Conducting the research |
| University of Birmingham research personnel | All data collected during study | Conducting the research |
| Newcastle University research personnel | Pupil dietary data (anonymised using ID numbers) | Owners of dietary survey software |
| Transcription company | Focus group and Interview audio files | Transcription |

**7. Lawful basis for processing:**

In this section we will record the lawful basis (or bases) required to fulfil the collection, processing and transfer of personal and sensitive data, in accordance with the Data Protection Act 2018 (The Act 2018) and the General Data Protection Regulation (GDPR).

The lawful bases for processing **personal** data are set out in Article 6 of the GDPR and at least one of these must apply whenever processing is to take place.

Predominantly, most research that is being conducted would fall under the following:

Article 6 (personal data) = (e) Public Task

This is because most of the research that we do here would have a perceived benefit to wider society and the public in general.

Article 9 (sensitive data) = (j) “Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes...”

This basis should be used as it will allow for the processing of sensitive data with the freedom required for research purposes.

There will be some instances whereby we cannot justifiably argue that there is clear ‘public interest’ in the research. This will more likely involve commercial research collaborations. For example, when we help to create new materials or software for commercial or private funders. In these instances, we may be required to use of another lawful basis, such as, (f) Legitimate Interests. However, if you are unsure, please contact the Information Compliance Unit (ICU) to discuss any queries you may have on this ([info.compliance@qub.ac.uk](mailto:info.compliance@qub.ac.uk)).

Article 6 (GDPR) Lawful Basis for Processing

Please tick the appropriate lawful basis:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal Obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone’s life.
5. **Public Task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you are processing special category data (sensitive data) you need to identify a lawful basis for processing **AND** a special category condition for processing. You cannot process sensitive data without satisfying one of the conditions below.

Article 9 (GDPR) Condition for Processing Special Category (sensitive) Data

Please tick the appropriate condition for processing:

**(a)**  The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

**(b)**  Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

**(c)**  Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

**(d)**  Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

**(e)**  Processing relates to personal data which are manifestly made public by the data subject;

**(f)**  Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

**(g)**  Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

**(h)**  Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

**(i)**  Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

**(j)**  Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued.

**8. Additional Information**

If there are any new technologies or systems of data collection and processing, which have not been used before or could be considered to impact expectations of privacy, please detail this here:

NA

If there are any other activities or processing taking place as part of this project that you feel may impact data privacy of participants, the public or other researchers and collaborators, please detail this here:

NA

**9. Identified Risks:**

Detail here the identified data privacy risks for the study. These will solely relate to the personal and sensitive data, the identified risks and the actions taken to mitigate risk. For example, a risk of unauthorised disclosure of participants’ health related data could be listed and a mitigating action would be to pseudonymise the data and ensure that it is stored in secure encrypted QUB storage facility.

|  |  |  |
| --- | --- | --- |
| Risk Identified | Mitigating Actions | Approved? (Y/N) ICU use only |
| Unauthorised disclosure of participant sensitive data | Data will be pseudoanonymised and stored in secure, password protected encrypted QUB storage facilities. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**10. Signoff and DPO Comments**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |