DETERMINANTS OF ADOLESCENT (NOW ADULT) SOCIAL WELL-BEING AND HEALTH STUDY (DASH)

PROPOSAL FOR ACCESS TO DASH DATA

(Please read our data sharing policy and guidance on completing this form before you begin)

Section 1: The Proposal

1.1. Title of the project

1.2. Anticipated start and end dates of project

Start | | End | |

1.3. Justification for using DASH data for this project.

In addition please attach a 1-2 page outline of your proposal which includes the hypotheses to be tested, methods of analysis planned, and justification for the specific variables requested.

Section 2: Research Governance

2.1. Lead External Researcher (designated PI)

Name
Institution
Address
Telephone
Fax
E-mail

2.2. Head of Department where DASH data will be held

2.3. Other external researchers involved in proposed project (and institutions)

2.4 Link Person

2.5 (Proposed) funder of research

Is funding for this proposal confirmed or pending a decision?

Confirmed ☐ Application Pending ☐ Application to be submitted ☐

If pending when is funder's decision expected? If still to be submitted when is the deadline for application?

2.6. Has this project been (or will it be) peer reviewed?

YES ☐ NO ☐

If so by whom?

Section 3: Data requirements

3.1. Data required

a) Which waves of data do you require?

Wave 1 (2002/03)	
Wave 2 (2005/06l)	
Feasibility (2012/14)	

b) Outline of variables required (More detailed information should be provided in your attached proposal).

3.2 Data confidentiality and security requirements

3.2.1 IS0 27001

If your organisation(s) have adopted IS027001 - Information Security - Security Techniques - Information Security Management Systems, please provide your certification number.

Organisation Name / Data Storage location	ISO 27001 Certification Number

3.2.2 Data Transfer and Storage Policies

MRC requires that all sensitive and person identifiable data is encrypted during transfer and whilst stored on mobile data storage devices and desktop and laptop computers.

- MRC prefers that any data provided is stored on secure networked drives as part of a secure managed server. If mobile data storage devices have to be used, you must implement adequate protection against device loss or theft, unauthorised interception and access .

- Where MRC supplied data is being stored on mobile data storage devices (for example but not limited to: USB 'sticks' and USB data storage drives, desktop or laptop computer) these devices must be fully encrypted to ISO/IEC 10118-3 certified level of security protection.
- Where devices cannot be encrypted (for example: CDs, DVDs) then the data must be encrypted to ISO/IEC 10118-3 certified level of security prior to storage on the mobile data storage device.

Please confirm that you have read and understood the details regarding MRC Data Transfer and Storage Policies by ticking here ☐

3.2.3 Data Storage

Please provide details on how and where you will store the data supplied by NSS. If data is being stored in more than one location then this section needs to be clearly completed for each location.

At what location(s) will data be stored? *Please list.*	
Will any data be stored outside of Scotland?	
If yes, please state the location outside Scotland where data will be stored. *Specific considerations will apply where data is stored outside of the European Union.*	

3.2.4 Storing of Data

This section relates to where data supplied by MRC will be stored.

Storage Device	**Please tick all that apply and specify for each, the location at which the data will be stored. *delete as appropriate.**	
	Confirm	**Location**
Networked server disk drive		
Networked desktop PC		
Standalone desktop PC*/ laptop*		
Mobile device		

Storage Format	**Please tick all that apply and specify for each, the location at which the data will be stored.**	
	Confirm	**Location**
Database		
Oracle database		
Microsoft Access database		
Microsoft SQL server		
IBM DB2		
MySQL		
Flat file e.g Excel spreadsheet, comma delimited file.		

3.2.5 Backup

Please confirm that your back up schedule is subject to the same security as the data provided by MRC for each location(s) that the data will be stored.

If not please provide details of your backup here:

3.2.6 Other Encryption or Anonymisation Procedures

MRC Data Transfer and Storage Policies require that all sensitive and person identifiable data is encrypted during transfer and whilst stored on mobile data storage devices and desktop and laptop computers to the standards outlined earlier. Please provide details of any other encryption or anonymisation procedures that may be used and at what stage.

Any other encryption or anonymisation procedures used	**At what stage**

3.2.7 User Access

Please provide details on user access and account management policies that you have in place to limit or prevent inappropriate access to the data supplied by MRC.

Will those accessing data, access it through individual or shared accounts?	**Individual**	**Shared**
Are 'complex' passwords (a mixture of alpha, numeric, upper/lower case, special characters) used on all accounts?		
How often are users required to change their passwords?		
Are procedures in place to regularly review user access to sensitive and potentially identifiable personal data?		
Are procedures in place to revoke user access to sensitive and potentially		

identifiable personal data when the user no longer requires this access?		
Will the data be accessed by staff working off site e.g. staff working from home?		
If yes, please detail how this access will be secured		
Please provide any additional details of how data provided by MRC will be protected from unauthorised access.		

3.2.8 Hardware Security

Please describe the physical security arrangements for the location where the data is to be stored e.g. this could be your computer department if the data is stored on a networked server, or may be where the PC/laptop holding the data is physically located.
Please describe the physical security arrangements for the location where the data is to be processed e.g. this is where your PC/laptop is located or wherever you are accessing the data from.
Please detail any protection that is implemented against the introduction of malicious software (e.g. computer viruses) in the areas where the data will be stored and processed.

Do your hardware replacement agreement(s) address how data are handled when hardware under warranty fails?	
If yes, would the hardware be returned to the supplier if there was a fault(s)?	

Please explain below how your organisation(s) dispose of hardware that they no longer require, that are faulty or covered by warranty.

If the data is being held in long-term archive(s) please explain how this data will be secured against further unauthorised access.
Who will have data management responsibilities for the data whilst in archive(s)?
What procedures are in place to retrieve the data from the archive(s)?

3.2.9 Data Retention and Disposal

Data should not be kept any longer than is necessary.

Please give details of your data retention policy for each of the organisations(s) holding the data, including any back-up copies.
Please give details of how the data, and any back-up copies, will be securely disposed of at the appropriate time by each of the organisation(s) holding the data.

Section4: Outputs

4.1 Please specify planned outputs from this project (publications, presentations, media contact, derived variables, other added value to DASH). Please note MRC policy requires all papers to be published in Open Access journals.

Section 5: Monitoring Progress

5.1 Please state how progress will be monitored

Each member of the proposed team who will have access to DASH data should sign a separate copy of this agreement and return it to the proposed link person. The lead applicant's copy should also be signed by their Head of Department and the link person.

Section 6: AGREEMENT FORM

The data in the DASH Study are highly confidential and have been given by respondents on the understanding they will be treated with the utmost confidentiality and respect. All users must ensure that respondents' confidentiality and the reputation of the study are safeguarded at all times.

Failure to uphold this agreement may result in all further access to DASH data by you and your team being denied.

Title of Project ……..

……..

Declaration

I have read the DASH data sharing policy and guidance on use of data by external researchers and agree to the conditions therein. ☐

I have also read and agree to abide by the requirements of the SPHSU's policies on data protection and confidentiality and on data management, by the MRC's guide to the handling of personal information in medical research, and by the MRC's guides to good research practice. ☐

I will not share the data with any third party other than those who have also signed this agreement. Nor will I attempt to match the dataset covered by this agreement with any other DASH data I currently hold. I will make no attempt to identify any individual within the study. ☐

I will keep the DASH link person, and DASH Steering Committee, informed of progress with the project and any issues that arise. ☐

I will obtain the prior consent of the SPHSU Director before submitting any papers for publication or presentation or have any media contact about results from DASH data. ☐

All papers based on DASH data will be submitted to Open Access Journals. ☐

At the end date of the project I will return all data, including documentation for any variables I have derived, and destroy all copies of the dataset I hold. ☐

Signature(s)

External Researcher ..... date.....

Link Person .....date.....

Sponsorship of research

I confirm that this institution is willing to act as joint sponsor of this research project with MRC SPHSU and will ensure the confidentiality, protection and appropriate ethical use and management of DASH data at all times.

Head of Department .....date.....

DASH Use only

Project Number …… Date agreed by Steering Committee ……..……..

Principal Investigator.....date……..

Collaboration approved

Unit Director……..…….…… date……..