Preface

This document has been developed for the purpose of the MVP of the dalink project.

This Information Sharing Protocol has been developed following consultation and working experience over a period of over 10 years by participating bodies, chiefly public authorities such as the Police, Health and Local Authorities.

1. Introduction

1.1 This document is an Information Sharing Protocol (for the purpose of this protocol, the terms data and information are synonymous). The aim of this document is to facilitate sharing of all personal, sensitive and non personal data between the public, private and voluntary sectors so that members of the public receive the services they need.

1.2 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal data is lawful, properly controlled and that an individual's rights are respected. This balance between the need to share personal data to provide quality service and protection of confidentiality is often a difficult one to achieve.

1.3 The legal situation regarding the protection and use of personal data can be unclear. This situation may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly.

1.4 There are fewer constraints on the sharing of non-personal data, that is data which either does not identify a living individual or when combined with other information that is in or may come into the organisation's possession will not identify a living individual.

1.5 Each partner to this protocol should ensure that all of their staff who are affected by it are

- aware of its contents and
- the obligations it and any information sharing agreements (ISA) which are created between the organisation signed up to it bring to them.

1.6 Each partner should also ensure that revisions to the protocol and ISA raised in it are signed in good time, which should be before any sharing takes place.

2. Scope

2.1 This overarching protocol sets out the principles for information sharing between Partner Organisations.

2.2 This protocol sets out the rules that all people working for or with the Partner Organisations must follow when using and sharing information.

2.3 This protocol applies to all information shared by Partner Organisations. Sharing is **not** restricted solely to information classified as Personal Data by the Data Protection Act 1998. This includes the following information:

a) All information processed by the organisations including electronically (e.g. computer systems, CCTV, Audio etc), or in manual records;
b) Anonymised, including aggregated data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.

2.4 This Protocol will be further extended to include other public sector, private and voluntary organisations working in Partnership to deliver services.

2.5 The specific purpose for use and sharing information will be defined in the Information Agreements that will be specific to the Partner Organisations sharing information.

3. Aims and Objectives

3.1 The aim of this protocol is to provide a framework for the Partner Organisations and to establish and regulate working practices between Partner Organisations. The protocol also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable legal purposes (see 6.3 and 11.5).

3.2 These aims include:

a. To guide Partner Organisations on how to share personal information lawfully.
b. To explain the security and confidentiality laws and principles of information sharing.
c. To increase awareness and understanding of the key issues.
d. To emphasise the need to develop and use Information Sharing Agreements.
e. To support a process that will monitor and review all information flows.
f. To encourage flows of information.
g. To protect the Partner Organisations from accusations of wrongful use of personal data.
h. To identify the legal basis for information sharing.

3.3 By becoming a Partner to this Protocol, Partner Organisations are making a commitment to:

a. Apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' Standards;
b. Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998;
c. Develop local Information Sharing Agreements (ISA) that specify transaction details.

3.4 Partner Organisations are expected to promote staff awareness of the major requirements of Information Sharing. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partners' Intranet sites and/or via other communication media.

4. The Legal Framework

4.1 The principal legislation concerning the protection and use of personal information is listed below and further explained in:

- Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Data Protection Act 1998
- The Common Law Duty of Confidence
- Computer Misuse Act
- Civil Contingencies Act 2004

4.2 Other legislation may be relevant when sharing specific information.

4.3 As part of each ISA, Partner Organisations should identify how they will meet its legal obligations and the legal basis (legislation and appropriate section(s)) under which information may be shared.

5. Information covered by this Protocol

5.1 All Information, including personal data and sensitive personal data as defined in the Data Protection Act 1998 (DPA).
In order to reduce the risks of DPA compliance and security breaches where possible anonymised data should be used.

5.2 Personal Data

5.2.1 The term 'personal data' refers to **any** data held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that

data.

5.2.2 The term is further defined in the DPA as:

- Data relating to a living individual who can be identified from those data;

or

- Any other information which is in the possession of, or is likely to come into the possession of the data controller (person or organisation collecting that information).

5.2.3 The DPA also defines certain classes of personal information as 'sensitive data' where additional conditions must be met for that information to be used and disclosed lawfully.

5.2.4 An individual may consider certain information about themselves to be particularly private and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

5.3 Anonymised Data

5.3.1 Organisations should ensure anonymised data, especially when combined with other information from different agencies, **does not** identify an individual, either directly or by summation.

5.3.2 Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed;
- The data cannot be combined with any data sources held by a Partner to produce personal identifiable data.

6. RESPONSIBILITIES WHEN Sharing Information

6.1 General

Each Partner Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.

6.1.1 Partner Organisations will ensure a reasonable level of security for supplied information, personal or non-personal, and process the information accordingly.

6.1.2 Partner Organisations accept responsibility for independently or jointly auditing compliance with the Information Sharing Agreements in which they are involved within reasonable time-scales.

6.1.3 Every organisation should consider making it a condition of employment that

employees will abide by their rules and policies in relation to the protection and use of confidential information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.

6.1.4 Every organisation should ensure that their contracts with external service providers include a condition that they abide by their rules and policies in relation to the protection and use of confidential information.

6.1.5 The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

6.1.6 Partner Organisations should have a written policy for retention and disposal of information.

6.1.7 Partner Organisations must be aware that a data subject may withdraw consent to processing (i.e. Section 10 DPA) of their personal information. In this case processing can only continue where an applicable Data Protection Act Schedule 2, and if relevant Schedule 3, purpose applies.

6.1.8 Where the Partner Organisations rely on consent as the condition for processing personal data then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to Partner Organisations and processing cease as soon as possible.

6.2 Personal Data

Personal data should only be shared for a specific lawful purpose or where appropriate consent has been obtained.

6.2.1 Staff should only be given access to personal data where there is a legal right, in order for them to perform their duties in connection with the services they are there to deliver.

6.2.3 This agreement does not give licence for unrestricted access to information another Partner Organisation may hold. It sets out the parameters for the safe and secure sharing of information for a justifiable **need to know** purpose.

6.2.4 Each signatory organisation to an ISA is responsible for ensuring every member of its staff is aware and complies with the obligation to protect confidentiality and a duty to disclose information only to those who have a right to see it.

6.2.5 Each signatory organisation should ensure that any of its staff accessing information under an ISA is trained and fully aware of their responsibilities to maintain the security and confidentiality of personal information.

6.2.6 Each signatory organisation should ensure that any of its staff accessing information under an ISA to follow the procedures and standards that have been agreed and incorporated within this Information Sharing Protocol and any associated Information Sharing Agreements.

6.2.7 Each Partner Organisation will share information in compliance with the principles set out at section 4 and any other obligations detailed in both the ISP and relevant ISA.

6.2.8 Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

6.3 Non-Personal Data

6.3.1 Partner Organisations should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the partner from whom the information originated from should be contacted before any further sharing takes place.

7. Restrictions on use of Information Shared

7.1 All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Information Sharing Agreement unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Therefore any further uses made of this data will not be lawful or covered by the ISA.

7.2 Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this should be considered when considering secondary use for non-personal information. If in doubt the information's original owner should be consulted.

7.3 Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc. Information about these will be included in the relevant ISA.

8. Consent – Applies to Personal Data only

8.1 Consent is not the only means by which personal data can be disclosed. Under the Data Protection Act 1998 in order to disclose personal data at least one condition in schedule two must be met. In order to disclose sensitive personal data at least one condition in both schedules two and three must be met.

8.2 Where a Partner Organisation has a statutory obligation to disclose personal data then the consent of the data subject is not required; but the data subject should be informed that such an obligation exists.

8.3 If a Partner Organisation decides not to disclose some or all of the personal data, the requesting authority must be informed. For example the Partner Organisation may be relying on a lawful exemption from disclosure or on the inability to obtain consent from the data subject.

8.4 Consent has to be signified by some communication between the organisation and the Data Subject. If the Data Subject does not respond this cannot be assumed as implied consent. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

8.5 If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.

8.6 Specific procedures will apply where the data subject is either not considered able to give informed consent itself because of either the data subject's age (Gillick Competency) or where the data subject has a condition which means the data subject does not have the capacity to give informed consent. In these circumstances the relevant policy of the Partner Organisation should be referred to.

9. INDEMNITY

9.1 Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

10. SECURITY

10.1 It is assumed that each Partner Organisation has achieved or will be working towards ISO 27001, the International Standard for Information Security Management, compliance or a similar level of compatible security. Partner Organisations should ensure that the minimum standards of security, that they require, are agreed with Partner Organisations with whom their information will be shared and included in the ISA. This should take account of the security classification of the information.

10.2 It is accepted that not all Partners will have security classification in place. .

10.3 Each partner signing this protocol and any individual signing the confidentiality agreement, agrees to adhere to the agreed standards of security. If there is a security breach in which information received from another party under this ISA is compromised, the originator will be notified at the earliest opportunity via the postholder identified at 3.2 of the ISA, who must forward details to the Information Security Section.

10.4 Where a partner has regular, specific security requirements, for example a corporate policy, either these or, if available, a hypertext link to the protocol should be included. This should help to avoid reviewing standards agreed previously when each new ISA is set up.

10.5 Security requirements will not be included in individual Information Sharing Agreements except where they are unique to that Agreement. This will ensure requirements are kept current, as notified, and avoid errors arising from having more than one copy of a Partner's standard requirements.

11. INFORMATION QUALITY

11.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and as up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result. Partner Organisations are expected to ensure that the Personal Data and Sensitive Personal Data that it holds is processed in accordance with DPA principles: this includes ensuring that the Data is accurate, complete and up-to-date and is not kept any longer than is necessary.

11.2 Where Partner Organisations share information under this Protocol it is expected that Partner Organisations will either have an Information Quality Strategy and the supporting processes and procedures in place or be formally working towards this.

11.3 All Partner Organisations are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this.

11.4 It is expected that all partner organisations will have or be working towards an organisational Information Quality Strategy. In generating and maintaining this policy due regard should be paid to the Information Quality Assurance Strategy.

11.5 Audit

Where a partner requires the ability to audit a Partner Organisation's Information Quality standards, for example as part of a Local Area Agreement (LAA) in which the receiving partner is the lead LAA partner, this and the obligations on the partners should be identified in the contract or ISA relevant to the sharing.

12. TRAINING

12.1 All Partner Organisations staff processing information shared under this Protocol and its associated ISA are expected to be trained to a level that enables them to undertake their duties confidently, efficiently and lawfully. This is an obligation on each Partner Organisation and responsibility for it cannot be assigned to another organisation, although delivery of training can with that third party's consent.

12.2 To minimise the costs associated with training and to ensure that all staff participating in activities based on information shared under a specific ISA it is strongly advised that partners collaborate in the development and delivery of training. Obligations and costs arising out of such collaborative working should be clearly identified in the ISA.

12.3 For the avoidance of doubt, where collaborative training is not adopted this should be stated in the ISA.

13. Individual Responsibilities

13.1 Every individual working for the organisations listed in this Partnership Agreement is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

13.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

13.3 Every individual has an obligation to request proof of identity, or takes steps to validate the authorisation of another before disclosing any information requested under this protocol and associated ISA's.

13.4 Every individual should uphold the general principles of confidentiality, follow the guide-lines set out in this Protocol and seek advice when necessary.

13.5 Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.

14. General Principles

14.1 The principles outlined in this protocol are recommended good standards of practice or legal requirements that should be adhered to by all Partner Organisations.

14.2 This protocol sets the core standards applicable to all Partner Organisations and should form the basis of all Information Sharing Agreements established to secure the flow of personal information.

14.3 This protocol should be used in conjunction with local service level agreements, contracts or any other formal agreements that exist between the

Partner Organisations.

14.4 All parties signed up to this protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law.

14.5 This protocol has been written to set out clear and consistent principles that satisfy the requirements of the law that all staff must follow when using and sharing personal information.

14.6 The specific purpose for use and sharing information will be defined in the Information Sharing Agreements that will be specific to the Partner Organisations sharing information.

15. Review Arrangements

15.1 This overarching agreement will be formally reviewed annually.

15.2 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

BMW ENERGY DATA SHARING POLICY

DOCUMENT CONTROL

Author	
Contributors	
Version	
Date of Production	
Date due for revision	
Post responsible for revision	

Primary Circulation list	
Number of document	
Restrictions	

CONTENTS

1. PURPOSE OF THE PROTOCOL

Local agencies are increasingly working together. To work together effectively, agencies need to be able to share information about the services they provide and the people they provide these services to.

This agreement has been developed to ensure Information Sharing for the purpose of the [INSERT NAME OF PROJECT/ACTIVITY], has an effective governance structure. The agreement has been produced to assist xxxxxxx and [INSERT PARTNERSHIP NAME] partners implement the required processes to [INSERT THE PURPOSE OF THE AGREEMENT] within the study design, across [DESCRIBE AREA / SCOPE OF PROJECT].

This agreement does not give carte blanche licence for the wholesale sharing of information. Information sharing must take place within the constraints of the law, relevant guidance, service specific requirements and is underpinned with the ethos of informed consent and client confidentiality being tantamount to any information sharing between agencies.

This protocol will be underpinned by the operational agreements as designed to meet the specific needs of the project study and to assure any information sharing is undertaken within the realms of current legislation and legal frameworks.

2. PRINCIPLES

Thus, this agreement outlines the principles and operational guidelines for how information and client data is securely managed across xxxx and [AREA NAME] partners to ensure the effective implementation and evaluation of the [NAME PROJECT / ACTIVITY].

The following key principles guide the sharing of information between xxxxxxxxxxxxxx and [AREA NAME] partners for the purpose of the [NAME PROJECT / ACTIVITY]:

2.1 Partner agencies endorse, support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymised information for the sole purpose of the [NAME PROJECT / ACTIVITY].

2.2 Agencies are fully committed to ensuring that if they share information it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.

2.3 All agencies have in place policies and procedures to meet the national requirements for Data Protection, Information Security and Confidentiality. The existence of, and adherence to, such policies provides all agencies with confidence that information shared will be transferred, received, used, held and disposed of appropriately.

2.4 Agencies acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of information from other agencies, employees and contracted volunteers will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures; any proposed

subsequent re-use of information which is sourced from another agency should be approved by the source organisation.

2.5 An individual's personal demographic information will only be disclosed to facilitate smooth implementation of the [PROJECT / RESEARCH]. For all other purposes, information must be anonymised.

2.6 Where information is shared, to facilitate the smooth implementation of the project only that which is needed and relevant will be shared. This will be on a "need to know" basis.

2. 7 Partner agencies will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard both to the confidentiality of information about people who are in contact with their agency and to the commitment of the agencies to share information.

2.8 All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.

2. 9 Partner agencies are responsible for putting into place effective procedures to address complaints relating to the disclosure of information, and information about these procedures should be made available to service users.

3. CONSENT

3.1 To facilitate effective success of the[INSERT NAME OF PROJECT / ACTIVITY], explicit client consent to participate is mandatory. As a **minimum**, individual participants will be informed that information will be shared across partner agencies.

3.2 For the purpose of this study consent will be sought [INSERT HOW CONSENT WILL BE SOUGHT], both written and verbal, being supported with written information regarding the [NAME OF PROJECT / ACTIVITY].

3.3 To assure explicit consent, the following must be sought from the participants:

- Consent to participate in the [PROJECT/RESEARCH]
- Consent for partner agencies to share both information and documentation across partner agencies and domains, in order to implement the necessary contacts required for the project
- Consent for information to be stored by [NAME OF RELEVANT ORGANISATION]
- Consent to be contacted by partner agencies from [NAME OF ORGANISATION], for the purpose of the project.
- Consent to the right to withdraw from the study at any point
- Further consent from participants (and on behalf of dependent family members) must be sought prior to any client information that would allow individuals other than those involved in undertaking the research to identify the client being included within the [NAME OF RESEARCH / ACTIVITY] (APPENDIX 1).

4. PROCESS

The project study comprises of [INSERT DETAILS OF THE PROJECT]. The initial contact to families / individuals will be made by [INSERT DETAILS OF THE PROJECT].

4.1.1 Data Collection

[DESRIBE HOW DATA WILL BE COLLECTED]. This will be used to [DESRIBE HOW THIS INFORMATION WILL BE USED / WHAT ARE THE INTENDED OUTCOMES]

[DESCRIBE IN DETAIL THE MECHANISMS FOR ACHIEVING THE ABOVE]

4.2 Data Storage

A completed [DESCRIBE DOCUMENTATION] will be entered onto a [INSERT NAME OF] database and thus shared with [WHO WILL HAVE ACCESS TO THE DATABASE].

Emergent themes will be analysed within the study evaluation stage and provide recommendations for future multi agency [WHAT WILL THE INFORMATION INFORM].

4.3 Data Sharing

As discussed, demographic information and data from [HOW WAS THE INFORMATION COLLECTED] will be shared with the [INSERT NAME OF] database. This agreement will ensure that partner agencies endorse the security and confidentiality constraints placed upon sensitive demographic information and data.

5. AUDIT AND REVIEW

All agencies accessing any client data must have appropriate governance and risk assessment measures in place, to assure the safe storage, access and utilisation of client identifiable data. Policies should be available for audit purposes with evidence of clear review dates.

Where not already in place, processes will be set up in each agency to adopt a risk management approach to breaches/problems in relation to the implementation of this agreement.

6. SUPPORTING POLICIES, PROCEDURES AND GUIDANCE

Supporting policies

For members of the public and staff from the agencies participating in the [PROJECT] to have confidence that information sharing takes place legally, securely and within relevant guidance, all agencies must demonstrate evidence of relevant policy guidance which meet the requirements for:

- Data Protection
- Confidentiality
- Information Security
- Caldicott principles

These policies must cover manual, verbal and computer-based information.

7. CONCLUSION

To assure the effective implementation and evaluation of the[INSERT TITLE OF RESEARCH / PROJECT], timely sharing of information is a key contributing factor.

This agreement acknowledges and provides a means whereby members of the public, staff and the agencies can be confident that where information is shared it is done so appropriately and securely for the sole purpose of the pilot and will not be utilised outside the scope of the project.