

2012

Information Sharing Agreement between Solihull MBC and the Safeguarding Adults Board

This Information Sharing Agreement is between Solihull Metropolitan Borough Council and partner members of the Solihull Safeguarding Adult Board. The Agreement addresses the legalities of sharing information and provides an overarching framework for the sharing of personal information for the purpose of safeguarding adults at risk within Solihull.

Contents

Version Control	2
1. Deciding what information needs to be shared.....	3
2. Fairness and transparency.....	9
3. Information quality standards	10
4. Retention of shared information	11
5. Security of shared information.....	12
6. Access to personal information and Freedom of Information.....	15
7. Review.....	16
Signatories.....	17

Version Control

Title: Information Sharing Agreement between Solihull MBC and the Safeguarding Adults Board

Version: 0.1

Document type: Draft

Prepared by: Solihull Metropolitan Borough Council and member organisations of the Solihull Safeguarding Adults Board

Approved by: Unapproved

Review date: Annually

Circulation: Signatory authorities to the Information Sharing Agreement

Version History		
Version Number	Date	Description
0.1	November 2011	Draft created and sent to SMBC and member organisations of the Solihull Safeguarding Board for comment
0.2	June - September 2012	Final revisions made to document. With Board members for signature.
0.3	October 2012	Final signed document.

1. Deciding what information needs to be shared

The Data Protection Act requires that any sharing of personal information must be necessary. Any information shared must be relevant and not excessive.

1.1 **Objectives**

- 1.1.1 This information sharing agreement sets out the principles for using and sharing personal information amongst the member organisations of Solihull's Safeguarding Adults Board.
- 1.1.2 To support earlier identification, prevention, investigation and treatment of abuse of vulnerable adults the Safeguarding Board is heavily reliant on all partner agencies sharing a variety of relevant information. Effective and structured sharing of information between partners has the ability to inform planning, allow for an understanding of trends and patterns of activity to be developed, to respond to emergencies and disasters appropriately, and to intervene and support the lives and safety of individuals, families and communities.
- 1.1.3 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. This must however be balanced with the need to share information to provide safe quality services, to protect individuals and the wider public and the protection of those individuals confidentiality.

1.2 **Risk Assessment**

- 1.2.1 There are considerable risks if information is not shared as has been identified in National Serious Case Reviews. Not sharing information could result in adults being left at risk of harm and mistreatment, which would have a negative or detrimental effect in the individual's health, wellbeing and safety.
- 1.2.2 The benefits to sharing information within the Safeguarding Adults procedures are effective and proportionate partnership working what will safeguard adults at risk. The benefits of sharing information within the Safeguarding Adults procedures outweigh the risk of not sharing information.

1.3 **Anonymised Information**

- 1.3.1 Wherever possible anonymised information should be used: In that, it is not possible to identify the individual from the information. However, there will be times within the Safeguarding Adults procedures where information must be client-identifiable – this will be any information, which can identify a living individual (either by itself or with other information likely to come into someone's possession).
- 1.3.2 The agency disclosing information has a right to expect that the agency receiving the information will treat it according to or under the same legal basis as which it was first provided to the disclosing agency.

1.4 Minimum Information Shared

- 1.4.1 Sharing excessive information that is surplus to requirements may breach the Data Protection Act. Therefore, only relevant information and the minimum necessary to achieve the objective will be shared. This applies to information shared internally and with partner agencies. It applies to information shared verbally, electronically, hard copies such as reports and access to information systems.
- 1.4.2 The ADASS Safeguarding Adults a National Framework of Standards 2005 and 2010 state that “there is an active duty to implement information sharing protocols“(An organisation that is party to this agreement) may disclose to any other (organisation that is party to this agreement) any information in its possession or control which it reasonably considers it should share with that body for the purposes of:
- (a) Identifying cases in which action may need to be taken in respect of matters arising in relation to the management of vulnerable adults.
 - (b) The consideration of issues relating to the taking of action in respect of such matters.
 - (c) The taking of action in respect of such matters.

Such information may include but is not restricted to data extracted from:

- A complaint or the analysis of complaints.
- An incident report or the analysis of incident reports.
- The files or results of an investigation into an incident or complaint.
- “Whistle-blowing” or other report of a concern relating to professional conduct or performance.
- The report or investigation of an alleged or actual criminal act relating to vulnerable adults.
- A report resulting from an inspection carried out by the regulator - Care Quality Commission.

- 1.4.3 Where a concern has been raised information may be shared that includes any of the above in addition to or contained within the following:

- Reports of a concern where evidence or information has been collated.
- The agenda, minutes and reports of a Vulnerable Adult Panel meeting
- Letters of referral to regulatory, indemnifying or representative bodies.
- Referrals to the police.
- Minutes of meetings of the Vulnerable Adult Board.

- 1.4.4 Personal information may include:

- The person’s name, and or any aliases they live under.
- The person’s address(s), occupation and date of birth.
- Information about the person’s social circumstances (which may include references to ethnicity).
- Information relating to the person’s alleged or proven, past or present criminal offences.
- The person’s movements, habits, conduct or practises.

1.5 Legal Provisions

1.5.1 **Powers to share information** - In order to share the information the signatories of this agreement need to be able to identify either express statutory powers or implied statutory powers, which underpin the exchange of information. Parties to this agreement have identified and agree that the following legislation underpins the sharing of the information.

1.5.2 Abuse that is a crime

- Common Law of Tort
- Crime and Disorder Act 1998
- Criminal Justice Act 1968
- Domestic Violence Crime and Victims Act 2004
- Family Law Act 1996
- Medicines Act 1969
- Offences Against the Person Act 1861
- Police and Criminal Evidence Act 1970
- Protection from Harassment Act 1997
- Public Order Act 1986
- Sexual Offences Act 1956
- Sexual Offences Act 1967
- Sexual Offences Act 2003
- Theft & Deception Acts 1968 and 1978
- Youth Justice and Criminal Evidence Act 1999

1.5.3 Provision of health and social care services

- Carer's (Recognition and Services) Act 1995
- Carers and Disabled Children Act (2000)
- Care Standards Act 2000
- Chronically Sick and Disabled Persons Act 1970
- Community Care (Direct Payments) Act 1996
- Disabled Persons (Service Consultation and Representation) Act 1986
- Employments Rights Act 1996
- Health and Social Care Act 1990
- Health Service and Public Health Act 1968
- Health Act 1999
- Housing Act 1985
- Housing Act 1996
- Housing Act 2004
- Local Authority Social Services Act 1970
- Mental Health Act 1959
- Mental Health Act 1983
- National Assistance Act 1948
- National Assistance (Amendment) Act 1951
- National Health Service Act 1977
- National Health Service and Community Care Act 1990
- Public Health Act 1936 and Public Health Act 1961
- Registered Homes Act 1984
- Registered Homes (Amendment) Act 1991

1.5.4 **Other relevant statutes**

- Court of Protection Rules 1994
- Data Protection Act 1998
- Disability Discrimination Act 1998
- Enduring Power of Attorney Act 1985
- Health & Safety at Work Act, 1974
- Human Rights Act 1998
- Mental Capacity Act 2005
- Power of Attorney Act 1971
- Public Interest Disclosure Act 1998
- Race Relations (Amendment) Act 2002
- Social Security (Claims and Payments) Regulations 1987

1.6 **Restrictions on sharing information**

- 1.6.1 Party's to this agreement have not identified any legislation that will prevent the sharing of the information.

1.7 **Sensitive Personal Information**

- 1.7.1 The threshold for sharing sensitive personal information is generally higher than for sharing other forms of information. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals. Sensitive personal information is defined as information relating to a person:

- (a) Racial or Ethnic Origin.
- (b) Political Opinions.
- (c) Religious Beliefs or other beliefs of a similar nature.
- (d) Trade Union Membership or Affiliation.
- (e) Physical or Mental Health or Condition.
- (f) Sexual Life.
- (g) Commissioned or Alleged Commission of Offences.
- (h) Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

- 1.7.2 Having considered the above, within Safeguarding Adults procedures it may be essential that this information is shared to allow partners to effectively work together to safeguard adults at risk.

1.8 **Consent**

1.8.1 Gaining the consent of the individuals' whose information you want to share will often help legitimise the sharing of personal information, however it is not always appropriate to use consent as the basis for sharing information, the following justifications under Safeguarding Adults may become applicable:

- **Serious harm**
It may be justified to share information where there is evidence that serious harm would be caused to the service user, (or another person) if this was not done.
- **Vital interests**
Information may be shared where this is in the "vital interests" of the service user or another person. This refers to life or death circumstances.
- **Prevention or detection of crime**
Personal information may be provided to the Police where this is necessary for the prevention or detection of crime. This is a power not an obligation. A judgement needs to be made in each case as to whether it is appropriate to release information taking into account the following criteria.
 - Without disclosure the task of preventing or detecting crime would be seriously prejudiced, and
 - Information shared is limited to what is strictly relevant to a specific investigation, and
 - There are satisfactory undertakings that the information will not be used for any other purpose than the specific investigation.

Advice should be sought, if there is uncertainty about interpreting this criteria.

- **Court Order**
Information must be shared where the service is instructed to do so by a Court (including a Coroner's Court.)
- **Legislation**
The law requires or permits the information to be shared.

Wherever possible and appropriate service users should be informed if their information is to be shared without consent.

Informed consent

1.8.2 If at any time it is decided that consent is needed, this must be a specific, informed and freely given agreement. In this context, a failure to object is not consent. Most importantly, the individual must understand what is being consented to and the consequences of giving or withholding consent.

Withdrawn consent

1.8.3 If consent is being relied upon to share information about a person, then sharing must stop if consent expires or is withdrawn.

Sensitive personal information

- 1.8.4 If the information to be shared is sensitive, then if consent is relied upon it must be 'explicit' consent. This difference between normal consent and explicit consent is that with explicit consent, the consent of the individual must be absolutely clear and ideally consent will be obtained in writing.

2. Fairness and transparency

The Data Protection Act requires that with some exceptions, in order for the information sharing to be 'fair' the individuals' whose information is being shared need to be made aware of the fact that the exchange is taking place, by whom and why.

2.1 **Fair Processing Notices**

- 2.1.1 The law says that the organisation in charge of processing personal information, so far as is practical should provide or make readily available the following information:

Identity – If it is not already apparent individuals must be informed of the name of the organisation / business area collecting the information along with contact details such as a telephone number.

Purposes of the Processing – It must be very clear why the information is needed and how it will be used. Providing this information means there will be no hidden surprises about how a person's information is used.

Note: Personal Information collected for one purpose must never be used for an incompatible purpose. Incompatible does not have to mean identical, but what it does mean is that you need to be able to provide a clear linkage between the original usage and the new proposed usage.

Anything else – Any other information necessary to enable the processing to be fair. Typically this will mean providing details of third parties to whom the information may be disclosed but there may be additional information you deem it important to inform people about also.

- 2.1.2 How you inform people of the above will depend upon the circumstances, for example, it might be a statement on a form, or it might be put on an organisations website or perhaps delivered verbally if circumstances warrant this.

Note: There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent for this. In many cases, a privacy notice will suffice. In cases where sensitive personal information is involved positive (often written) consent will be needed.

- 2.1.3 Members of the Safeguarding Board agree to ensure that when collecting information from individuals they provide the information described above.

3. Information quality standards

The Data Protection Act requires that personal information be relevant, kept accurate and up to date. Decisions taken on inaccurate information can have serious consequences.

3.1 Six Elements of Information Quality

3.1.1 Signatories to this agreement have no desire to share inaccurate information. Parties are in agreement that any information shared should be of the highest quality and that procedures / systems will be in place to guarantee this. The 6 elements to Information Quality agreed upon are:

- 1. Accurate** Information should be sufficiently accurate for its purposes. The need for accuracy must be balanced with the importance of the uses for the information, and the costs and effort of collection. Sometimes it may be acceptable to have some degree of inaccuracy. However, where compromises have to be made on accuracy, this should be made clear.
- 2. Valid** There may be national or local rules to follow. Different organisations may record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mismatched or becoming corrupted. Before sharing information you must make sure that the organisations involved have a common way of recording key information.
- 3. Reliable** The methods used to gather information should remain consistent as users of the shared information need to be confident that any differences reflect real change rather than differences generated by different collection methods.
- 4. Timely** Information should be shared as quickly as possible after being captured else it may become out of date and obsolete. The speed and frequency at which you share the information will depend upon how likely it is to change over time.
- 5. Relevant** Information should be relevant to the purposes for which it is shared. The accuracy of information and methods used to collect/generate it may be excellent and fulfill all parties' needs today, however, tomorrow, there may be new requirements or rules introduced that have to be adhered to and mean that you have to review the information collected.
- 6. Complete** Information requirements should be clearly specified. Methods of collecting the information need to meet these requirements else the information may be incomplete. It is vital that those responsible with collecting or creating information are all clear about why the information is being shared and the purposes it will be used for else the wrong information might be shared.

4. Retention of shared information

The Data Protection Act requires that personal information should not be kept for any longer than is required.

- 4.1.1 Parties to this agreement understand that the information shared should not be held indefinitely and should only be retained for as long as it is needed. The retention period will either be based upon legislation, which requires that the information be kept for a set period, or in the absence of any legislative requirement, each party to this agreement will determine how long they need to keep the information based upon their own business need.
- 4.1.2 After this time the information will be permanently deleted and this will apply both electronic and manual records.
- Electronic Records – For information to be deleted it must be permanently and irrecoverably deleted. This means it cannot exist on the organisations electronic backups or other systems, unless it is held for different purposes, which require it to be retained for longer.
 - Manual Information – Each party to this agreement holds manual information on service users. Each service user has a manual file (similar to a personnel file). In line with the above retention schedule each party has agreed that the file will be shredded and put into confidential waste at the end of the retention period
- 4.1.3 It is perfectly permissible for parties to this agreement to have different requirements for how long they keep the information shared. This is because different organisations will be working under different legislation or have differing business needs.

5. Security of shared information

The Data Protection Act requires that organisation's have adequate organisational and technical safeguards in place to guarantee the safety and security of personal information they hold. Any safeguards must be proportional and appropriate to the nature of the information and the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage.

5.1 **General principles**

5.1.1 Members of the Safeguarding Board agree that personal information shall be protected by appropriate technical and organisational measures including the agreement that:

5.2 **Identify/Evaluate Risk**

5.2.1 Information to be shared is generally highly sensitive and the damage that could result by accidental loss or disclosure is significant. Therefore, a high level of security and safeguards needs to be in place to manage the risk of accidental loss or disclosure.

5.3 **Protective Markings**

5.3.1 A difficulty that can arise when information is shared is that the various organisations involved can have different standards of security and security cultures. Adopting the Government Protective Marking Scheme can help organisations involved in the sharing of information to make sure there is consistency when handling personal information.

5.3.2 Due to the sensitive and confidential nature of Safeguarding Adults information the Government Protective Marking of RESTRICTED should be applied to the information shared. This is on the basis that loss or misuse would:

- Pose a risk to an individual's personal safety or liberty.
- Facilitate the commission of, or impede the investigation or prosecution of low level crime.
- Directly lead to a risk to an individual's personal safety (e.g. the compromise of the address of a victim of abuse, where there is a reasonable risk of further abuse if such information became known).
- Cause either prolonged distress for an individual, or short term distress or significant embarrassment for many individuals.

5.3.3 Any information shared should be clearly marked as RESTRICTED

5.4 Physical Mechanisms for delivering/sharing the information

Electronic Sharing of Information

- 5.4.1 Any information that is shared electronically must be done so via encrypted means. For example if information is shared by email then it will not be sufficient to simply password protect a document, the email itself must be encrypted. Alternatively, the email can be sent via a secure network such as the GCSX network.
- 5.4.2 If information is shared by copying it onto portable media such as a CD, DVD or memory stick then the media must be encrypted and protected by a strong password containing at least 8 characters in length and containing upper and lower case characters and at least one special character and one number.

Postal Service

- 5.4.3 If information is sent through the post it will be sent by special delivery. Items sent by Special Delivery are tracked throughout their journey through the postal system and so if they get lost there is a stronger chance they will be found. Items sent by Recorded Delivery is treated as normal post except for the fact they are signed for upon delivery. Therefore Recorded Delivery will not be used.
- 5.4.4 Parties to this agreement will ensure that the envelopes/packaging used are either special tamper proof packaging or else strong enough to prevent damage and potential loss of information during transit.

5.5 Indemnity Agreement

- 5.5.1 Each party will keep each of the other party or parties fully indemnified against any and all costs, expenses and claims arising out of any breach of the Information Sharing Agreement, particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending party or parties or its subcontractors, employees, agents or any other person within the control of the offending party of any information obtained in connection with this agreement.

Individuals who cannot be covered by the Indemnity Clause

The signatories to this agreement agree that the organisations they represent have joint and equal responsibility for ensuring that where individuals are privy to the shared personal information yet are not covered by the indemnity clause that they are required to sign a confidentiality agreement.

- 5.5.2 In respect of every disclosure, the receiving party undertakes to indemnify the disclosing party against all actions, claims, demands and proceedings and all damages, costs and expenses incurred in connection therewith made or brought against the other party by any person in respect of any loss or distress to that person by the loss, unauthorised destruction, or disclosure of any personal information by the party which has been disclosed to them in confidence by the other. "disclosure of any personal information" also includes "any disclosure found to be in contravention of the Data Protection Act 1998".

- 5.5.3 Provided that this indemnity shall not apply where the liability arises from information supplied which is shown to have been incomplete or incorrect (i.e. where the information does not comply with the fourth data protection principle) unless the partner claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part.
- 5.5.4 Further this indemnity shall not apply unless the partner claiming the benefit of this indemnity notifies the granting partner as soon as possible and no later than [seven] days from the date that gives rise to any action, claim or demand to which this indemnity applies of such action, claim or demand, permits the granting partner to deal with the action, claim or demand by settlement or otherwise and renders the granting partner all reasonable assistance in so doing.
- 5.5.5 This indemnity shall not apply to the extent that the partner claiming the benefit of the indemnity makes any admission which may be prejudicial to the defence of the action, claim or demand. By signing this Information Sharing Agreement all parties and signatories agree that they have read, understood and agree to abide by the terms and conditions of this agreement.

6. Access to personal information and Freedom of Information

The Data Protection Act gives individuals the right to ask for and receive copies of personal information held by an organisation (subject to certain exemptions) and the Freedom of Information Act gives individuals rights of access to all other types of information.

6.1 How to Handle requests Information

- 6.1.1 All parties to this agreement have agreed that if either organisation receives a request from an individual to access any of the shared information it is their responsibility to process the request. However, should the information in question have originated from the other organisation then they will be contacted within 5 days of receiving the request and views sought on whether the information should be disclosed or whether there are any reasons which would legitimise it being withheld.
- 6.1.2 If a member of the public requests a full copy of the signed information sharing agreement, neither party to this agreement have any objections to a full copy being released. Both parties to the agreement would ordinarily make this information available in any case by way of their publication schemes.

7. Review


7.1 Annual Reviews


7.1.1 This Information Sharing Agreement will be reviewed by all parties on the anniversary of the signing of this agreement. Thereafter, it will be reviewed at least annually or sooner should circumstances warrant it.


7.1.2 Each review will examine whether:

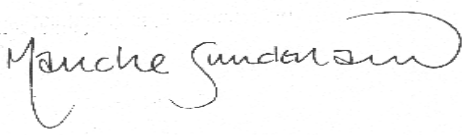
- The sharing of information is having the desired effect.
- Fair processing notices still provide an accurate explanation of the information sharing activity.
- Procedures for ensuring the quality of information are being adhered to and are working in practice.
- Organisations you are sharing information with are also meeting agreed quality standards.
- Retention periods are being adhered to and continue to reflect business need.
- Security remains adequate and, if not, whether any security breaches have been investigated and acted upon.
- Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.

Signatories

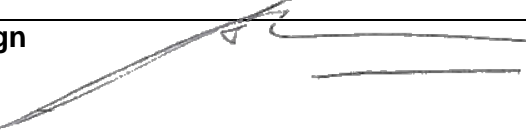
Solihull MBC	Name Ian James
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 12 July 2012

West Midlands Police	Name JEAN YOUNG
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 11.10.12

Solihull CCG	Name Sue Roberts Chief Nurse
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 31st October 2012

Heart of England NHS Foundation Trust	Name Mandie Sunderland
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 18.5.12

Staffordshire and West Midlands Probation Trust	Name Sarah Chand
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 9.7.12

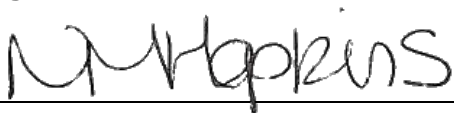
Birmingham & Solihull Mental Health NHS Foundation Trust	Name DAVID NEWNAM
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 9 / 10 / 2012

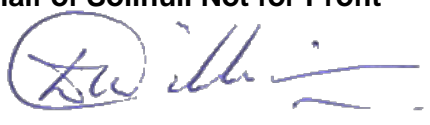

Coventry & Warwickshire NHS Partnership Trust	Name Roisin Fallon-Williams Director of Business Transformation (SIRO)
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 28 September 2012

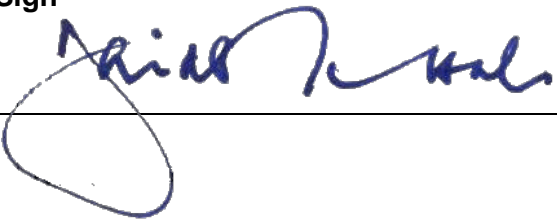
Solihull Community Housing	Name John King
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 01 June 2012 (original) 18 September 2012 (Adrian Thomas)

West Midland Ambulance Service	Name Sandy Brown
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 8 November 2012

Age UK Solihull	Name ANNE F HASTINGS
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date: June 2012

Solihull Action through Advocacy	Name Nicky Hopkins
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 21/9/12

On behalf of Solihull Not for Profit Group 	Name DAVID WILLIAMS
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 18/10/12

On behalf of Community and Voluntary Sector	Name DAVID MATTOCKS
I have read the Information Sharing Agreement and on behalf of my organisation I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement	
Sign 	Date 12 th October 2012

