INFORMATION SHARING AGREEMENT (ISA) (FOR THE SHARING OF PERSONAL DATA)

BETWEEN

NOTTINGHAM CITY COUNCIL

TRADING STANDARDS SERVICE

AND

AGE UK NOTTINGHAM & NOTTINGHAMSHIRE

VERSION CONTROL

Title: Information Sharing Agreement (ISA) Template
Current version: 3.0
Document Type: Paper and electronic
Prepared by: Stephanie Pearson, Information Governance Specialist
Approved by: Information Management and Strategy Group
Approval date: August 2014
Review date: Annually
Circulation: All employees

Document revision dates:

Revision	Date	Revision description
Version 1	August 2013	ISA Template created.
Version 2	May 2014	Minor revision
Version 3	August 2014	Annual revision with GBC colleagues

Acknowledgements

This Information Sharing Agreement has been adapted from the Nottinghamshire Police Information Sharing Agreement to meet local Nottinghamshire requirements. We are grateful to the Information Management Unit of Nottinghamshire Police for giving permission for the Nottinghamshire Police Information Sharing Agreement to be amended in this way and Nottingham City Council and Gedling Borough Council for their hard work in adapting the documentation for use by other public organisations.

SUMMARY SHEET

ISA TITLE :	SCAMS HUB PROJECT

Background and Summary	**Background and summary** **Why do we need to share information?** The aim of this document is to facilitate the lawful exchange of information between public, private and voluntary sectors, so that members of the public retain the confidence they need in the organisations they trust, whilst receiving the services they require in a convenient and timely manner. 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 services and the need to protect the confidentiality of information is often a difficult one to achieve. 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. There are fewer constraints on the sharing of non-personal data, which is data that 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. Each partner to this Agreement 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.

PARTNERS	NOTTINGHAM CITY COUNCIL AGE UK NOTTINGHAM & NOTTINGHAMSHIRE

Date Agreement comes into Council:	

Date of Agreement Review:	Six months after coming into force, then annually

Agreement Owner:	NOTTINGHAM CITY COUNCIL

Agreement drawn up by:	JANE BAILEY

Location of Signed Agreement within Council:	Trading Standards, 3rd Floor, Central Police Station, North Church Street, Nottingham, NG1 4BH

CONTENTS

1. INTRODUCTION

1.1 This Agreement has been developed to facilitate partnership working between the Council and the identified partner agency. This Agreement identifies the legal powers and methods of sharing information in order to achieve common goals for the benefit of the Nottinghamshire area.

1.2 The Council is committed to partnership working, and continually looks for opportunities to work more closely with local identified partners. Organisations involved in providing services to the public have a legal responsibility to ensure that the use of personal data is lawful, properly controlled and that the individual's rights are respected. This balance between the need to share personal data to provide quality services and the protection of confidentiality is often a difficult balance to achieve.

1.3 In adopting this partnership approach it is important that the policies/practices of the agencies involved complement each other to ensure that any action taken is appropriate, necessary, proportionate and consistently applied. Collaborative working takes place for a variety of reasons which include in the interests of public safety, child protection, and for the prevention, detection and reduction of crime.

1.4 This Agreement outlines the need for the Council and the agency involved to work together **to protect elderly and vulnerable residents against scam crime** in the Nottinghamshire area and provides a framework for action.

1.5 Each partner to this Agreement should ensure that all of their staff who are affected by it are aware of its contents and the obligations it creates between the organisations signed up to it.

2. PURPOSE AND BENEFITS

2.1 In order to prevent elderly and vulnerable Nottingham City residents from falling victim to scam crime, Trading Standards will share information of individuals identified as at risk to Age UK Nottingham and Nottinghamshire.

2.2 Effective information exchange is the key to partnership working. The effectiveness of information exchange is a reflection of the effectiveness of the partnership as a whole.

2.3 The general power of competence in the Localism Act 2011 enables local authorities to do anything that an individual may do, provided the act is not specifically forbidden in the 2001 Act or by another statute.

2.4 The Crime and Disorder Act 1998 and the Police Reform Act 2002 places obligations on various agencies as defined in the legislation to

co-operate in the development and implementation of a strategy for addressing the issues relating to crime and disorder in their area.

2.5 The Agreement is designed to:

- Help promote information sharing;
- Minimise the risk of breaking the law, and reduce any associated reputational risks caused by the inappropriate or insecure sharing of personal data;
- Gain better public trust by ensuring that legally required safeguards are in place and complied with;
- Provide better protection to individuals when their data is shared;
- Provide colleagues with a better understanding of when it is appropriate and acceptable to share information without peoples knowledge or consent or in the face of objection;
- Support action in accordance with any of the legislative provisions of the Crime and Disorder Act 1998 and Data Protection Act 1998 where personal data is included;
- Govern the use and management of information provided by the parties to this agreement;
- Assist with the exchange of information to support other crime reduction activities;
- Document the specific purposes for which the signatory partners have agreed to share information;
- Describe the roles and structures that will support the exchange of information between partners;
- Set out the legal gateway through which the information is shared, including any reference to the Data Protection Act 1998 (DPA), the Human Rights Act 1998 (HRA) and the Common Law duty of confidentiality;
- Describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities included under the DPA and any partner specific security requirements;
- Ensure compliance with individual partners' policies, legal duties and obligations;
- Ensure that the Council and its partners comply with the Information Commissioner's Code of Practice on Data Sharing.

3. PARTNER(S)

3.1 This Agreement is between the following partners:

NOTTINGHAM CITY Council ("the Council") of;
Loxley House, Station Street, Nottingham, NG2 3NG
and

AGE UK Nottingham & Nottinghamshire, of;
Bradbury House, 12 Shakespeare Street, Nottingham NG1 4FQ

Referred to collectively in this Agreement as "the Partners".

4. POWER(S)

4.1 This Agreement fulfils the requirements of the following legislation:

- The Local Government Act 1972
- Crime and Disorder Act 1998
- Police Reform Act 2002
- Localism Act 2011
- Data Protection Act 1998

5. INFORMATION SHARED

5.1 **The Council** agrees to share the following information:

The names, addresses and telephone numbers of individuals in the Nottingham City area, who have been identified as potential victims of scams

The information will be disclosed in the following data format:
A secure password protected spreadsheet will be shared with the Age UK Scams Project Manager. The password for the secure spreadsheet will be shared verbally with the Age UK Scams Project Manager over the telephone.

The information shall be exclusively used for the following purposes:
To engage with the individuals identified and

* Confirm whether the person is a victim of scams

* Obtain intelligence from the victim

* Support the victim

* Safeguard the victim for the future

5.2 **Age UK Nottingham & Nottinghamshire** agrees to share the following information:

Feedback to Nottingham City Trading Standards on

* Whether a response has been received from the resident

* Whether the resident is a victim of scams

* Intelligence from residents in relation to the perpetrators, the methods used and the profile of the victims

* Support given to residents

* Safeguarding carried out with the victim for the future

The information will be disclosed in the following data format:
A separate feedback form for each individual referred to Age UK to be hand collected from Age UK Nottingham & Nottinghamshire's office on Shakespeare St.

The information shall be exclusively used for the following purposes:

- Reporting to the National Scams Team
- Building a profile on scam criminals affecting Nottingham City residents
- Building a profile on consumer behaviour & which/ how/ why residents are affected by scams

5.3 All information held by either organisation to be shared under this Agreement is covered by this Agreement. I.e. this Agreement covers all information, including personal and sensitive data as defined in the Data Protection Act 1998 (DPA). In order to reduce the risks associated with data sharing, consideration should always be given to whether the need can be fulfilling by the sharing of anonymised data. If so, anonymised data should be used wherever possible.

5.4 **Personal Data**

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. 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).

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. An individual may consider certain information about them 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.

5.5 **Anonymised Data**

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

5.6 Partners are responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Agreement.

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

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

5.9 Partners 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.

5.10 Parties 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.

5.11 Partners should have procedures in place to report misuse, loss, destruction, damage or unauthorised access, suspected or otherwise, of information. 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 supplied under this Agreement.

5.12 Partners should have a written policy for retention and disposal of information and any information supplied in reliance on this agreement should be governed by these rules.

5.13 Where Partners 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 the other Partner and processing cease as soon as possible.

5.14 Partners 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.

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

5.16 Employees 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.

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

5.18 Partners should not assume that 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.

5.19 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. RESTRICTIONS ON THE USE OF INFORMATION SHARED

6.1 All shared information, personal or otherwise, must only be used for the purpose(s) specified in clause 5 of this 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 this ISA.

6.2 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.

6.3 Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc. Specific restrictions are: NONE

9.3 All information sharing agreements shall be reviewed by the Trading Standards Manager who will identify whether the completion of a full or small Privacy Impact Assessment (PIA) is required.

9.4 No information provided under this Agreement shall be disclosed to a 3rd party without the explicit consent of the Partner disclosing the data. Requests must be made in writing to the Information Governance team of the GIS, Data and Information Service.

9.5 Where this Agreement covers any social care information, the Caldicott Guardian must also be consulted over the information sharing being proposed and must sign their agreement.

9.6 Personal data shall be processed in accordance with the rights of Data Subjects under the Data Protection Act:

- Each Partner will ensure it has an appropriate registration with the Information Commissioner's Office covering the types of data it holds and the ways in which these data are processed.
- Partners will respond to any notice from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.
- Partners are responsible for responding appropriately to Subject Access Requests addressed to them and to providing information to the Data Subject to enable them to make appropriate requests to other Partners where appropriate.
- Data Subjects have the right to object to processing. How the Data Subject makes such objections should be detailed in each Partner's Privacy Notice. It is the responsibility of Partners to produce and maintain their own Privacy Notice.
- Partners are responsible for responding appropriately to Freedom of Information Act 2000 (FoIA) and Environmental Information Regulations 2004 (EIR) requests addressed to them. Where appropriate the Partner receiving the request should consult the other prior to making any decision surrounding disclosure, although ultimately any decision as to what will/will not be disclosed rests with the party who received the request.
- Subject Access - is an individual's right to have a copy of information relating to them which is processed by an organisation. If a Partner receives a Subject Access Request and the personal data is identified as belonging to the other agency or data controller, it will be the responsibility of the Partner receiving the request to contact the other, usually the Data Protection Officer/Information Governance team who will take the lead as far as the request is concerned. Communication must take place speedily thus allowing the servicing of the request to take place within the statutory 40 calendar day, time period.

10. STORAGE, RETENTION AND DISPOSAL

10.1 Partners must ensure that they have appropriate measures in place to ensure the secure storage of all information provided under this Agreement as follows:

- Information provided should be held in a lockable storage area, office or cabinet.
- Electronic files must be protected against illicit internal use or intrusion by external parties through the use of appropriate security measures.

10.2 Any information held by the Partner will be disposed of, in line with the Council's retention and disposal schedule or returned to the SPOC, when no longer required at the cessation of the Agreement or at the request of the Council.

10.3 The information provided under this Agreement shall not be kept any longer than necessary and if requested by the Partner providing the information must be returned to it, destroyed or erased (including all copies whether paper or electronic). The information shall be destroyed in an appropriate manner, as follows:

- All electronic data must be destroyed in an appropriate manner which renders it irretrievable. This could be logically, physically, digitally or magnetically destroyed.
- All paper documents should be immediately strip shredded or incinerated.

11. DISCLAIMER

The Partner disclosing the data disclaims all liability to the Partner receiving the data in connection with the use of data supplied under this Agreement and shall not, under any circumstances, be responsible for any special, indirect or consequential loss or damages including but not limited to loss of profits arising from the use of the data by the Partner receiving the data.

Information shared by the Council may include intelligence which may not have been corroborated but all other detail will be relevant and believed accurate at the time of obtaining it until proven otherwise. Any false allegation will still be retained as an accurate record of fact.

12. INDEMNITY

The Partner receiving the data shall indemnify the Partner disclosing the data in full in respect of any loss or damage caused to the Partner

disclosing the data as a consequence of the unauthorised disclosure of data supplied under this Agreement.

13. INFORMATION QUALITY

13.1 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. Partners are expected to ensure that the Personal Data and Sensitive Personal Data that they hold are 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.

13.2 Partners 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.

14. TRAINING

14.1 Partners' employees processing information shared under this 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 Partners and responsibility for it cannot be assigned to another organisation, although delivery of training can with that third party's consent.

14.2 To minimise the costs associated with training and to ensure that all staff participating in activities based on information shared under this ISA partners may collaborate in the development and delivery of training.

15. AUDIT

15.1 Either partner has the power to audit the other to ensure compliance with the provisions of this Agreement.

The Partner conducting the audit shall:

- provide at least 5 Working Days' notice of its intention to conduct an audit, unless prevented from providing such notice by Law;
- comply with security, sites and facilities operating procedures applicable to any sites or information being audited;
- use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the other Partner; and

- bear its own respective costs and expenses incurred in respect of the audit.

15.2 The Partner who is the subject of the audit shall:

- grant to the Partner conducting the audit and their respective authorised agents the right of reasonable access to relevant records, sites and materials and shall provide all reasonable co-operation and assistance; and
- shall bear their own respective costs and expenses incurred in respect of compliance with its obligations under this clause.

16. REVIEW AND TERMINATION

16.1 This ISA will be reviewed 6 months after its initial draft then yearly thereafter.

16.2 This review is the joint responsibility of the partners and should be carried out by officers named in clause 18 in consultation with the SPOC.

16.3 Any Partner can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and be evidenced. Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this Agreement, or their nominated representative. This meeting to take place within 14 days of any suspension. Termination of this Information Sharing Agreement should be in writing to the other Partners giving at least 30 days' notice.

17. SINGLE POINT(S) OF CONTACT (SPOC)

17.1 Each partner will appoint a SPOC who will be a manager of sufficient standing with a co-ordinating and authorising role.

17.2 The specific responsibilities of the SPOC are:

- Ensure compliance with the policies and procedures outlined in the Appendices to this Agreement;
- The information exchanged is kept secure and confidentiality is maintained as appropriate to the information's level of protective marking as defined by the Data Controller;
- Deciding on a case by case basis if and why a public interest overrides a duty of confidence;
- Ensuring any changes to the SPOC are confirmed in writing;
- Professional, ethical standards are maintained;
- The Data Protection Principles are upheld;
- Appropriate staff training is provided on this Agreement; and
- Adequate arrangements exist to test adherence to the Agreement.

17.3 **Nottingham City Council Single Point of Contact (SPOC):**

Name: **JANE BAILEY**

Position: TRADING STANDARDS MANAGER

Email: **jane.bailey6909@nottinghamshire.pnn.police.uk**

Tel: 0115 8445018

17.4 **Age UK Nottingham & Nottinghamshire Single Point of Contact (SPOC):**

Name:

Position:

Email:

Tel:

18. SIGNATURES

18.1 By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purposes of this Agreement and compliance with all relevant legislation.

18.2 It is the responsibility of all signatories to appoint appropriate SPOCs to manage the performance of this Agreement.

18.3 **Authorised Signatory for Nottingham City Council Head of Service/ Trading Standards**

Name: Jane Bailey

Position: Trading Standards Manager

Signed: Jane Bailey **Date:** 23rd November 2015.

18.4 **Authorised Signatory for Nottingham City Council Information Governance/Management colleague**

Name:

Position:

Signed: N. Pollard **Date:** 24/11/2015.

18.5 **Authorised Signatory for Age UK Nottingham & Nottinghamshire:**

Name:

Position:

Signed:_____ **Date:**

18.6 **Authorised Signatory for Age UK Nottingham & Nottinghamshire Information Governance/Management colleague**

Name: MICHELLE ELLIOTT

Position: ASSISTANT CHIEF EXEC (RESOURCES)

Signed: MElliott **Date:** 2/12/15

19. APPENDIX A – DESIGNATED AUTHORISED STAFF

Confidentiality Agreement

In signing the following I understand that information exchanged will only be used for the purpose for which it was requested and it will be securely stored and destroyed when no longer required. Any agency and its employees becoming recipients for the purpose of this information exchange process will, upon signing this Agreement, be bound by its terms and conditions.

DESIGNATED AUTHORISED STAFF

Name	Contact Details	Signature

Please continue on another sheet if necessary.

Designated Authorised Staff/ Management Co-ordination

The SPOCs will be responsible for providing the Trading Standards Service at the Council with the contact details of the 'Designated Authorised Staff'. Designated Authorised Staff will be those who, after being subject to the Council's disclosure and barring requirements, will have access to the information shared under this Agreement. A list of Designated Authorised Staff will be made available within these documents. Failure to adhere to this may result in a temporary suspension of information sharing with the Council.

Notification of Moves and Changes of Staff

The SPOCs will be responsible for maintaining the list of 'Designated Authorised Staff' ensuring that it is current and that any required amendments are completed. A new and revised list of Designated Authorised Staff will be submitted to the Council every six months via the SPOC at the Council so that they may update their records of staff with access information under this Agreement. The new document will include the signatures of the Designated Authorised Staff named within it.

Vetting

Disclosure and Barring (DBS) checks will only be undertaken by the Council where the current roles held by designated staff and any resultant DBS check performed does not adequately cover the types of information being accessed, or where a DBS check would be required if the person is operating in a role substantially similar to that held by a council employee where a DBS check would need to be undertaken. (i.e. social and health care information).