External Ref:	HIG
Review date	June 2013
Version No.	SafetyNet V1.1 FINAL
Internal Ref:	NELC

Humber Information Sharing Charter

This Charter may be an uncontrolled copy, please check the source of this document before use. Refer to the 'Strategy and Policy Register' or Humber data observatory website (www.humberdataobservatory.org.uk) for the latest version.

NORTH EAST LINCOLNSHIRE COUNCIL www.nelincs.gov.uk	Maintenance and control of the Charter is undertaken by North East Lincolnshire Council on behalf of the Humber Information Governance Group, all enquiries should be addressed to transparency@nelincs.gov.uk

Contents

Humber Information Sharing Charter

Tier 3 - Operational Management Information Sharing Agreement for the community safety SafetyNet PRIME system

Humber Information Sharing Charter

Tier 3 - Operational Management Information Sharing Agreement for the community safety Unilink SafetyNet system

1. Introduction

Introduces the Agreement, linking to the Tier 1 Charter and Tier 2 Protocol.

The partnership recognises the importance of confidentiality to service users. It is essential to the effective running of the whole partnership. A 'service user' is anyone who approaches the partnership for help, advice and information, along with those engaged in any of the partnership agencies or satellite services.

This Tier 3 information and data sharing protocol is made under Humber Information Sharing Charter (Tiers 1 & 2) and applies to:

The following statutory community safety partnerships and their agencies as defined in Appendixes A and B of this protocol for the sharing of information together with Unilink Software Ltd. for the secured storage of the shared information:

- Safer Neighbourhoods North Lincolnshire
- Safer Communities North East Lincolnshire
- *(if the other Humber CSP's wish to license this system their details can be inserted here)*

The ISP has been agreed between the participating partner organisations.

Partners have given consideration to its contents when drawing up this document.

The functions which this information sharing protocol community are seeking to support involve:

A system will be maintained to store information concerning personal cases (the Integrated Case Management system) and a linked facility covering the recording and resolution of neighbourhood problems (the Neighbourhood Management system). The system will use customer insight to build intelligence concerning people residing within the Humber community safety partnership areas, understanding their needs and know how to engage with them:

- In order to join up different agencies with a safeguarding responsibility

- Provide the ability to highlight risk trends at an individual level in order that safety partnership teams can prioritise actions before situations escalate

- Enable victims of crime or violence, persons suffering from the effects of anti-social behaviour and vulnerable people identified as being at risk of anti-social behaviour to feel better supported by triggering the appropriate assessment process as risks

begin to escalate (also a joint provision within the operation of the Victim & Vulnerable Persons Index system).

- Information shared will enable the victims of crime to choose whether they wish to participate in restorative justice processes

- Information shared will case manage the perpetrators of crime and anti-social behaviour.

- Provide a system for the recording, monitoring and resolution of neighbourhood problems and tensions concerning community safety based on the recommended police National Intelligence Model methods (SARA – Scanning, Analysis, Response and Assessment and PAT – problem analytical triangle [Victim, Offender, Location]).

This information may also be shared to support the effective administration, audit, monitoring, inspection of services and reporting requirements. Partners may only use the information disclosed to them under this ISP for the specific purposes set out in this document.

Personal information shared to support functions other than those detailed above are not supported by this ISP.

Service Users included in this ISP

The Service Users which this ISP relates to include:

- Citizens who reside within Humber community safety partnership areas.

- The perpetrators of crime, anti-social behaviour or victimisation who are not resident within the Humber community safety partnership areas but undertake their activities within the partnership's area.

Benefits to Service Users

Benefits to Service Users include:

- Pro-active assessment of their risk of becoming a victim of crime, violence and anti-social behaviour

- Providing intelligence for the community safety partnership about the offenders of crime and anti-social behaviour to inform the partnerships early intervention strategy and make the partnership more responsive and effective in reducing crime and anti-social behaviour

- Provide community intelligence to inform the partnership about crime and anti-social behaviour activities within a neighbourhood in support of the 'Community Trigger' proposals developed by the Home Office.

Details of personal information being shared

Personal information shared for the purpose of this ISP includes a range of information regarding the Service Users needs.

The information may include:

For responsible agencies detailed within Tier 2 of the Humber Information Sharing Charter concerning community safety partnerships

- A person's name, address and contact details or other such property or personal identifiers that will assist with maintaining the accuracy of the system.
- Linked case information such as witnesses, family member details and their relationship with the data subject.
- Personal contact and engagement event diary information concerning agency staff, members of supporting community and voluntary groups, Neighbourhood Action and Area Action team member details.
- Information relating to consultations, engagements, surveys, visual environmental audits, etc. that may be collected from members of the public in the operation of the system.
- Structured information detailed in the system's data dictionary described in Appendix C.
- Unstructured (e.g. free text e-mails, word documents, photographs and other images, etc.) that may be generated and stored within the system:

For community and voluntary support organisations or individuals providing support as detailed in Appendix B.

- At the discretion of the system data controller and with the agreement of the community safety partnership's senior management restricted access to the system facilities may be provided to other organisations and individuals not described as responsible authorities in the Crime & Disorder Act 1998.

The information is used to support the operation of the Unilink SafetyNet system (Integrated Case Management and Neighbourhood Management modules).

Only the minimum necessary personal information consistent with the purposes set out in this document must be shared.

Key Identifying information

When sharing information name, address, contact details, property identifiers (such as the NLPG Unique Property Reference Number) and personal identifiers (such as the National Insurance Number) will be used were available, to ensure that all partners are referring to the same Service User.

The Role and Responsibility of Partners

The responsibility for the release or sharing of information remains with the contributing partnership agency's data controller or officer supplying the information.

Appendix B lists additional organisations, bodies and individuals (such as GPs) that information may need to be shared with on a need-to-know basis. Normally offender information will not be shared with these other bodies, information relating to victims may be shared if the detailed and appropriate consent has been sought and obtained from the Service User before it is released to these other users.

2. Legislation

The specific legislation allowing the sharing of information, referencing the Tier 2 Protocol

The provisions of the Crime & Disorder Act 1998 and subsequent legislation as detailed in the Humber Information Sharing Charter (Tier 2, Sub section 8) covering the activities of the statutory community safety partnerships.

3. Data Controllers

Who the Data Controllers are

The data controllers are the delegated responsible officers identified for each community safety partnership's areas for the:

- Integrated Case Management system
- Neighbourhood Management system

Responsible officers may change over time. A document will be maintained and posted onto the SafetyNet system's portal detailing these officers for each area (refer to Section 7 below).

4. Information Format and Quality

- *The format and detail of the information to be shared*
- *Procedures for Quality Assurance*

The format and details of the data dictionary supporting this system are described in Appendix C of this protocol document.

The approved collection tools for partner organisations to gather the personal information detailed in this ISP are:

- Partnership organisation's system applications, their business processes and operating procedures, electronic and paper-based forms supporting these procedures.
- Similarly, other multi-agency partnership system applications operated by the Humber community safety partnerships including the Victim & Vulnerable Person Index system and any other supporting software applications.
- Data is maintained in real-time within the system. Data supplied through system interfaces may be subject to batch operations.
- Any inaccuracy in the information supplied should be reported to the data controller of the appropriate responsible agency. The data controller of the organisation supplying the data is responsible for the information and will need to take appropriate steps to correct any inaccuracies.

5. Information Security and Confidentiality

- *The procedure for making requests and the arrangements for access to information and restrictions including those for third party access*
- *The storage standards*
- *The retention and destruction arrangements*
- *The procedures in place for the secure transfer of data*

Breaches of security, confidentiality and other violations of this ISP must be reported in line with each partner organisations' incident reporting procedures.

Data exchanges between partner organisations and the data centre will be undertaken by the most secure means that is consistent with their own internal technical procedures and supporting infrastructure. If the responsible authority is connected into the appropriate Public Service Network (Police National Network, Government Connect or NHS N3 network) then routing data exchanges and uploads through this secure and nationally accredited network is the preferred option. Responsible authorities must put plans into place to submit the appropriate network change requests enabling data processing and exchanges through this option at the earliest opportunity. The minimum standard for the exchange or uploading of data to the data centre will be by the use of the secured file transfer protocol (SFTP).

Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared.

The SafetyNet system and its supporting software applications will be stored in a secured data centre provided by Unilink Software Ltd. The data centre will be hosted in a facility that has been accredited by the Hampshire Police force information security section. The continuing operation of application will be dependent on the accreditation of the data centre being maintained by the operator.

The governance of any data or derived information stored with Unilink Software Ltd remains with the originating Humber community safety partnership and its contributing agencies.

Unilink Software Ltd together with any sub-contactor(s) they may employ do not have any rights to operate with the supplied data except to configure, test and operate the system applications that set up and maintain the system and its interfaces. The Humber community safety partnership derived data used to demonstrate the application's facilities or support the supplier's sales and marketing efforts must be changed sufficiently so that it does not reference an actual living person residing within the Humber sub-region.

Information governance procedures will be agreed between responsible authorities for the archiving and subsequent, deletion, destruction and disposal of personal information relating to the operation of the SafetyNet system within agreed timeframes.

6. Client Consent to Share Information

- *Details of the consents required including obtaining consent, withdrawal of consent, disclosure without consent*
- *Privacy / Fair Processing Notice requirements*

Client consent provisions are as detailed in the Humber Information Sharing Charter (Tier 2 – Common provisions of the Strategic Purpose protocols) and any exceptions and legal gateways that apply to the operation of community safety partnerships. Privacy and the fair processing of data are also covered by this section.

If the community safety partnership operates the Victim & Vulnerable Person Index system as well as the SafetyNet system then the Victim & Vulnerable Person's consent may be obtained through the Index system's pre-registration consent process either by their completion of a paper based form or electronic means such as a web form or mobile phone application. Ideally, the citizen's consent should be obtained prior to data processing within this system but if this is not pre-registered then their consent for the further processing of their data should be obtained at the earliest opportunity.

Consent registrations already collected by the victim risk assessment processes undertaken within the operation of the Index system or other multi-agency or single agency case management systems will also be regarded as the citizen's pre-registration of consent for their information to be processed by the Unilink SafetyNet system.

7. Roles and Responsibilities for the Sharing of Information

The lead officers for each signatory organisation and the specific roles and responsibilities within the organisation, including sub organisations

The lead officer and any other roles and responsibilities of the contributing responsible agencies are to be detailed in the SafetyNet system portal.

8. Monitoring/Review

The specific arrangements in place to review the agreement and handle complaints.

Each partner organisation has a formal procedure by which Service Users can direct their complaints regarding the application of this ISP

Review of this ISP

This ISP will be reviewed 22nd. June 2013 or sooner if appropriate.

9. Signatories

The signatories to the agreement.

Signatories for the community safety partnership responsible and relevant agencies participating in this protocol are detailed in the accompanying signatory forms. These forms will create Appendix A of this protocol.

Signatories for participating cooperating bodies such as community and voluntary organisations are detailed in Appendix B of this protocol

Signatories for Unilink Software Ltd, 7 West Links, Tollgate Business Park, Chandlers Ford, Eastleigh, Hampshire, SO53 3TG covering the data centre hosting, operation and maintenance of **SafetyNet:**

.....  .....

Appendix A – SafetyNet partnership agency signatures

The Safer Neighbourhoods partnership agency signed forms will form Appendix A of this protocol. This appendix covers the responsible and relevant agencies contributing to the operation of this protocol for the SafetyNet system application.

Appendix B – Other organisations or individuals

Cooperating bodies i.e. community support, voluntary organisations or responsible individuals (such as GPs) that SafetyNet information may be shared with as described in the Home Office national support framework guideline document. The participation of cooperating bodies and the level of access to their staff will be decided upon by the SafetyNet steering group.

Organisations and individuals signatories may be appended to each of these Appendixes when they decide or are invited to participate in the operation of this protocol.

Appendix C – SafetyNet data dictionary

Following on from the general specification of the protocol described above this appendix details the data dictionary supporting the SafetyNet system i.e. the data tables and elements contributing to the shared information contained within the system. This appendix takes the form of a separate document supplied by Unilink Software Ltd.