SENTINEL – INFORMATION SHARING AGREEMENT (ISA)

SUMMARY SHEET

PURPOSE	To facilitate the exchange of information between partners to adopt a multi-agency approach to tackling anti-social behaviour to identify vulnerability and reduce the risk, threat and harm to individuals.

PARTNERS	Blaby District Council Charnwood Borough Council Charnwood Neighbourhood Housing (not ISP signatory) Harborough District Council Hinckley and Bosworth Borough Council Leicester City Council Leicestershire County Council Leicestershire Police Melton Borough Council North West Leicestershire District Council Oadby and Wigston Borough Council Rutland County Council

Date Agreement comes into force:	10th October 2011

Date of Agreement Review:	10th October 2012

Agreement Owners:	Senior Information Risk Owners of partners set out above

Agreement Drawn up by:	Anne Chafer and Michael Hopkins

Protective Marking:	Not Protectively Marked

VERSION RECORD

Version No.	Amendments Made	Authorisation	Date
0.1	Draft submitted to project oversight board	n/a	21st July 2011
0.2	Amendments following ICO visit and further information re schedule 2 and schedule 3 conditions moved to main body of document	n/a	28th July 2011
1.0	Responses to comments made on v0.2 by partners	Submitted to project oversight board on 2nd September 2011for approval subject to any minor corrections	26th August 2011
1.1	Minor amendments agreed at project oversight board and correction to section 4	Version for signing by partners	12th September 2011
1.1.1	Corrections requested by Leicestershire Police	n/a	14th October 2011

1. Policy Statements and Purpose of this Information Sharing Agreement

1.1 Purpose and Justification for Information Sharing

The purpose of this Agreement is to facilitate the exchange of information, in order to ensure that business objectives are met and to comply with the statutory duty placed on local authorities and the police as 'responsible authorities' to work together to develop and implement a strategy and tactics for reducing crime and disorder, anti social behaviour and substance misuse. In particular the need has been identified to share information between Partners to adopt a multi-agency approach to tackling anti-social behaviour to identify vulnerability and reduce the risk, threat and harm to individuals and adopt integrated approaches to facilitate appropriate service delivery.

The Sentinel system will provide an anti-social behaviour IT system operating across the whole of the Leicestershire Police force area which is deployed at each of the Partners. It will enable reports of anti-social behaviour incidents to be logged on a single system which is made available to users in real time, with appropriate safeguards regarding user access, throughout the force area. This will enable subsequent events to be responded to appropriately with regard to the risk, threat and harm to the individual and Partners to more effectively identify patterns of behaviour and hotspots for focused attention. The system will also enable the development of more consistent approaches to recording incident and investigation information and a reduction in the duplication of interventions enabling an effective incremental approach to be adopted.

The success of Sentinel will be monitored within each Partner's geographical area through the normal operation of local community safety partnerships. The Anti-social Behaviour Strategy Group, which covers the whole of the area across which Sentinel is deployed will also monitor the effectiveness of Sentinel, for example in terms of the number of multi-agency interventions and improvements to the tactical assessment information provided to the Anti-social Behaviour Joint Action Groups.

1.2 Governance

This Agreement sits under the over-arching County Information Sharing Protocol agreed in July 2009 which lays out broad principles for the sharing of information. This document will be signed by all organisations that will become users of the system in the roll out of Sentinel.

The Partners will be joint data controllers of the data for the normal operation of Sentinel because they act together to decide the purpose and manner of any data processing. As a result the Partners are jointly liable for the processing. The Agreement therefore sets out the responsibilities of the individual Partners with respect to the data they provide and use. Where information stored on Sentinel is used other than for the common purpose described above the Partners will not be considered as joint data controllers but data controllers in common and each

Partner will, therefore, be individually liable for the processing they undertake. Further information is set out in section 3.8.

A list of the Partners and their identified Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs) can be found in the Sentinel Risk Management and Accreditation Document Set.

2. Legal Basis for Information Sharing

This Agreement has been developed to achieve the purposes/objectives as set out in Section 1 above. It is the intention that all aspects of information exchange and disclosure relating to this Agreement shall comply with relevant legislation that protects personal data.

Specific steps have been identified to ensure that the Agreement complies with legislation that protects personal data. These are set out in Appendix A. Each data controller is responsible for putting those steps in place and for any breaches of this Agreement which occur through failure to do so.

Further information relating to the requirements of the Human Rights Act 1998 is set out in the Information Sharing Protocol.

Identifying a lawful basis will enable Partners to defend a challenge with regard to the Data Protection Act 1998 and/or the Human Rights Act 1998 and is necessary for compliance with principle 1 of the Data Protection Act. A lawful basis may be provided by common law, statute or legal precedence supported by Home Office guidance or professional/executive bodies, e.g. Dept of Health, Association of Chief Police Officers, Dept of Education, etc. The following section identifies statutory gateways for information exchange that apply to the Partner agencies for the purpose of this Agreement.

Police

The Police Act 1996 gives police constables certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment when ever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.

The police also have a general common law power to disclose information for policing purposes.

Local Authorities and Police

Section 115 of the Crime and Disorder Act 1998 confers a power on any person to disclose information to a relevant authority (which are the police, local authority, health authority and probation service or to any other person acting on behalf of such authority, e.g. Charnwood Neighbourhood Housing) which is

necessary or expedient to help implement the provisions of the Act, which include contributing to local strategies to reduce crime and disorder, seeking anti-social behaviour orders and consultation prior to seeking such orders.

Section 10 of the Children Act 2004 places a duty on Children's Services Authorities to make arrangements to promote co-operation between itself and relevant Partner agencies to improve the well-being of children in their area and for the police and other local authorities to co-operate in those arrangements.

Section 11 of the Children Act places a duty on local authorities and the police to make arrangements to ensure that their functions are discharged with regard to the need to safeguard and promote the welfare of children.

Local Authorities

Section 2 of the Local Government Act 2000 enables local authorities to do anything to promote social, economic, or environmental well-being in their area provided that it is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out such activities they have regard to their sustainable community strategies.

In addition Section 111 of the Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions

3. Information

3.1 What data is it necessary to share?

Personal Data

Personal data is information which relates to any living individual who can be identified from the data or from the data and other information held by the data controller. Additional guidance is given in the Information Sharing Protocol. Section 2 above sets out the statutory gateways under which personal data may be exchanged for the purposes of operating Sentinel.

Sensitive Personal Data

This is also defined in the Information Sharing Protocol and includes information on the commission or alleged commission of offenses by the data subject, proceedings for any such offence and the disposal of such proceedings, the racial or ethnic origin of the data subject and the physical or mental health of the data subject. The Data Protection Act sets out additional safeguards for any processing of sensitive personal data.

The personal data and sensitive personal data to be shared through the Sentinel system has been identified as that necessary to enable the effective multi-agency case management of anti-social behaviour incidents. As such it is proportionate

and the minimum amount needed to achieve the purpose identified in Section 1. The data to be shared are set out in Appendix B and the specific steps to ensure that the processing of the data through this Agreement meets the requirements of the Data Protection Act are set out in Appendix A. Flowcharts describing how information sharing will operate on a practical basis can be found in Appendix D and these will be expanded upon to produce a practical guide for users of the Sentinel System.

3.2 Who is going to be responsible for sharing this information and ensuring information is accurate?

Each Partner will identify an Information Asset Owner (IAO) who is responsible for the day-to-day management of the sharing of information through the Sentinel system at their organisation. IAOs should be managers of sufficient seniority to be able to take decisions about the use of Sentinel in their organisations and understand what information is held, how it is used and transferred, and who has access to it and why, in order for Sentinel to operate within an acceptable level of risk.

This person is also responsible for the accuracy of any information entered on Sentinel by that organisation and ensuring that copies of the Agreement are made available as necessary within their organisations to ensure adherence to it. A list of IAOs can be found in the Sentinel Risk Management and Accreditation Document Set.

It is not necessary for the IAO to be a user of Sentinel. Further details of the different user groups and their roles within the Sentinel system are set out in section 3.5.

3.3 How is this information going to be shared?

The Sentinel software system provides access to a single web-based database which will initially cover Leicestershire Constabulary, the seven District Councils within the county, Leicester City Council and Rutland County Council plus the Leicestershire County Council Youth Offending Service and Charnwood Neighbourhood Housing. The system utilises a single core Sentinel product, hosted on a dedicated server provided by Rackspace on behalf of Vantage Technologies (the company that owns Sentinel) via which information can be accessed and shared in real time using an internet connection. Access rights to the information stored on Sentinel is based on the allocation of users to one of five user groups as set out in section 3.5 and Appendix B.

Section 3.8 sets out the circumstances other than the sharing functions provided by the Sentinel system itself under which information will be shared. The information contained within the Sentinel system has been given a protective marking of Restricted. The main implications of this in relation to the security of information sharing other than through the internet-based system are set out in the table below.

Issue	Appropriate Security
Creation of records, e.g. printing	All records to be protectively marked as Restricted.
Storage and disposal of paper records	Protected by a locked container within a secure building/room. Use secure waste sacks for disposal by incineration or shredding, protected as above when left unattended.
Transfer of paper records within a Partner organisation	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.
Transfer of Partner records outside Partner organisation	By secure post or courier, requiring a signature on delivery, in a sealed envelope. **Do not** show protective marking on the envelope.
Sharing of information via e-mail	Only via secure e-mail e.g. pnn or gcsx.
Sharing of information via fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.
Sharing at multi-agency meetings	This must be for a specific purpose and should only be made to attendees not covered by this Agreement at the meeting on a need to know basis. The disclosure and reason must be included in an appendix to the minutes and only circulated as a 'Restricted' document. The Chair of such meetings has responsibility for ensuring compliance with these requirements. Appendix C contains guidance for Chairs and a confidentiality agreement for use at such meetings.

3.4 How will you keep a record of what information has been shared?

Every record entered on Sentinel is authored and date-stamped and each incident has an identified lead officer. The lead officer is likely to be one of the operational users of Sentinel (see section 3.5) and will be responsible for co-ordinating the investigation into the reported anti-social behaviour incident and, once that investigation is concluded, for recommending to the relevant enhanced user (see section 3.5) that the case is closed.

Any updates and amendments to Sentinel records are also authored and date-stamped. The Sentinel system also creates an audit log of reports generated through the search function and the printing and exporting of search results. As a safeguard against improper use of the system, monitoring of use will be undertaken.

Any disclosures of information held on the Sentinel system except as set out in this Agreement will be recorded by the administrator at the organisation concerned along with details of the justification for that disclosure. The Security and Change Management Control Group will receive reports on all such disclosures so that any patterns or trends can be identified. The reports will include details of the volume of and reasons for disclosures.

3.5 Who will have access to this information and what may they use it for?

The following table sets out the different levels of access that will be provided for users of the Sentinel system. Each Partner is responsible for identifying the appropriate user group for each of its users on a least privilege basis.

User Group	Approximate no. of users	Description of access
Basic User – Basic Users are likely to be administration staff who may only log new complaints	25	These users will be able to add a skeleton record which includes: details of the initial contact; description of the incident and details of the people involved (complainant/ victim/perpetrator/witness) with a brief entry made on the working sheet. They will be able to send a trigger email alert to another person, alerting them to the fact that a record has been created and needs to be responded to. Once they have submitted the record, they will be unable to view it again or to amend it. They will not be able to see any other records and they will have no search capability.
Operational User – these will be the bulk of front line staff Operational Users are likely to be Police Beat Officers, General Response Officers, ASB Case Officers, Housing Officers and Community Safety Officers	750	These Users will be able to add comprehensive new complaints, including: details of initial contact; detailed description of the incident, details of the people involved (complainant/victim/perpetrator/witness), including Risk Assessments where appropriate. They will be able to add comprehensive working sheets and record specific actions taken along with recording ASB interventions/disposals. They will be able to update records which they have put on themselves and records which have been put on by other users relating to incidents in the geographical area of their organisation. They will be able to send a trigger email alert to another person, alerting them to the fact that a record has been created and needs to be responded to or to make a request for information or to raise a task. They will be able to upload and attach relevant documents to a record. They will be able to submit their cases to supervisory officers (normally Enhanced Users) seeking consent to close. They will be able to carry out basic search functions

User Group	Approximate no. of users	Description of access
		from within the complaint forms but not via use of the Ad-hoc reporting function (see the footnote regarding Police Officer use).
Enhanced User – are likely to be Police Sergeants, Community Safety Managers/ASB Coordinators and Housing Managers	40	These users will have all of the capability that Operational Users have. In addition they will have a manager function which allows them to view cases submitted for closure along with the ability to close a complaint/case.
Super User/Analyst	24 – With the exception of Leicester City Council, each local authority will be limited to one officer with this capability. The number of Super Users/Analysts at the City Council will be determined closer to their go-live date on the basis that it will be the minimum possible number. The Police may have up to 10 users of this type.	These users are unlikely to be individuals who need to be able to add a new complaint or update/amend an existing complaint. For that reason, whilst they will need to understand how this the process works, they will not be routinely given add or amend rights (because of the dual role performed by some staff at district level there may be a need to give a small number of these users add or amend rights and this can be arranged where necessary). These Users will be given access to a module called Ad-hoc reporting. It will enable them to conduct comprehensive and global searches for information across the entire county system. For this reason, numbers of these Users have been kept to a minimum and operating procedures and on-screen reminders make clear the limited circumstances under which such searches are appropriate. The Ad-hoc reporting function also enables auditing of use of the system by users. Use of the Ad-hoc reporting tool will be evaluated after 12 months of operating the Sentinel system to determine whether there is a continued need for local authority users to conduct searches outside their authority's area.
Administrator	16	These staff will have full capability with the Sentinel System. They will have all the rights that Basic, Operational, Enhanced and Super Users. In addition they will be responsible for enabling New Users, having first confirmed that they meet the relevant code of connection. They will be able to set new passwords. These Users will first have to have completed Training Level 2 or 3 before being trained as an Administrator. Administrators are likely to be senior managers at local authorities and may be IT Specialists within the Police Force.

Note re Police Users – Regardless of the user group in which they sit all police users will have access to records held in all of the Districts, Rutland and the City.

3.6 How securely does the information need to be stored?

Standard security requirements are detailed in the Information Sharing Protocol.

In addition, the Sentinel system has gone through an accreditation process as set out in the Government's Information Assurance Standards 1 and 2. This has resulted in the production of an appropriate code of connection for Partners and security operating procedures for use of the system. Each Partner signing this Agreement and any individual signing the security operating procedure agrees to adhere to the agreed standards of security.

3.7 How long are you going to keep the data?

In the first instance information will be retained, through being stored on the dedicated Sentinel server hosted by Rackspace and accessed as described in this Agreement, in accordance with the policies and procedures of Leicestershire Police. This approach will be reviewed after 12 months of operating the Sentinel system with the aim of producing a retention policy specific to Sentinel. The Sentinel system allows records to be flagged as either suitable for automatic deletion or requiring human intervention before a decision to delete is taken. Reports can also be run using the Ad-hoc reporting function to identify inactive records.

3.8 Further Use of Information

The following further or secondary uses of the information held on the Sentinel system have been identified which relate to or support the purpose set out in section 1.1.

- Use of the information outside of the sharing functions provided by the Sentinel system itself for purposes which are necessary to achieve the primary purposes set out in section 1.1, for example consideration of anti-social behaviour cases at steering groups or similar meetings and the forwarding of papers to legal practitioners
- Forwarding information to Victim Support – only with the consent of the data subject
- Forwarding personal information for the purposes of hate incident monitoring – only with the consent of the data subject
- Providing information required for the Common Assessment Framework process
- Forwarding anonymised information for analysis and assessment purposes.

In addition to these purposes, it has been agreed that:

- Leicestershire Police will use the Genie search tool to search data stored on Sentinel. Leicestershire Police will only use the information on the

Sentinel system for other policing purposes responsibly and proportionally and where this is justified by the risk of harm to the public

- Leicester City Council will consolidate data stored on Sentinel with data stored in their Enterprise Reporting System to help them to identify vulnerable and 'at risk' members of the public as well as the perpetrators of Anti-Social Behaviour. Leicester City Council will only use the information from the Sentinel system for this purpose responsibly and proportionally and where this is justified by the risk of harm to the public.

Where the disclosure of personal information held by one of the Partners is identified as being necessary for the prevention or detection of crime or apprehension or prosecution of offenders and failure to do so would prejudice the purpose, the data controller can release the necessary information under Section 29(3) of the Data Protection Act 1998. This Section provides an exemption to unlawful disclosure on a case by case basis for the holder of the information, provided the disclosure is necessary for the purpose. Any such disclosures should be recorded in accordance with section 3.4.

In the cases described in the two paragraphs immediately above, data processing will not be in conjunction with the purpose set out in section 1,1 and, as set out in section 1.2, each Partner will be individually responsible for the data processing it undertakes.

Partners will not use information stored on the Sentinel system otherwise than set out in this Agreement nor will they disclose the information other than when required to do so by law.

4 Breach of confidentiality

Partners will follow the following procedure if there is a breach of this Agreement by a Partner or a third party who has received information under this Agreement. Examples of breaches include, but are not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or the system.
- Changes to information or data or system hardware, firmware, or software characteristics without proper authorisation or consent.
- Unwanted disruption or denial of service to the system.
- The unauthorised use of the system for the processing or storage of data by any person.

Any breaches of this Agreement must be reported to the Partner providing the information, the Leicestershire Police Information Security Officer and the Chair of the Security and Change Management Control Group. The Leicestershire Police Information Security Officer and the Chair of the Security and Change

Management Control Group will log all breaches and initiate any relevant investigation. The outcome of any investigation will be circulated to all Partners.

Disciplinary procedures must be invoked against any member of staff found to have been responsible for the breach by the employing Partner, with the Information Commissioner being notified of the breach and any action taken if the breach is serious. Leicestershire Police will determine whether any criminal investigation is required.

To ensure that lessons are learnt from incidents and to improve the response process, the Security and Change Management Control Group will receive reports on all reported incidents so that any patterns or trends can be identified. The reports will include details of the volume and types of incidents and the results of any investigation.

5 Indemnity

Signatories to the Information Sharing Protocol have already indemnified other signatories.

Charnwood Neighbourhood Housing will keep each of the other Partners fully indemnified and each of the other Partners will keep Charnwood Neighbourhood Housing 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.

6 Individuals who cannot be covered by the Indemnity

The parties to this Agreement understand that there may be individuals present at certain meetings who are not employed by an organisation and therefore are not in a position to sign this Agreement due to the liability of the indemnity.

In order to ensure that the data controllers who are supplying personal information to the meeting fulfil their duties under the Data Protection Act 1998 and that the principles are complied with, it is recommended that the first time any individual attends a meeting covered by this Agreement is required to sign a confidentiality agreement as set out in Appendix C. The responsibility for ensuring that this takes place and for retaining the signed copies lies with the Chair of the meeting.

7 Review of Information Sharing Agreements

This Agreement will initially be reviewed after 6 months and 12 months and then as necessary following the guidance in the Information Sharing Protocol.

8. Closure/termination of Agreement

Any Partner organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and be evidenced. If necessary, steps will be taken to restrict access to the system as soon as possible after such a request.

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 or withdrawal from this Agreement should be in writing to all other Partner organisations giving at least 30 days notice.

9 Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

Each Partner organisation shall publish this Agreement on its website and refer to it within its publication scheme. If a Partner organisation wishes to withhold all or part of this Agreement from publication it shall inform the other Partner organisations as soon as is reasonably possible. Partner organisations shall endeavour to reach a collective decision as to whether this Agreement is to be withheld from publication or not.

All recorded information held by public sector agencies is subject to the provisions of the FOIA and the EIR. Information requests made under the FOIA or the EIR will be co-ordinated and responded to by the organisation receiving the request in relation to the whole of the Sentinel system to the extent that this is relevant to the request. Even where there is no requirement to consult with third parties in responding to requests for information, the parties to this ISA will consult the parties from whom information originated or relates to and will consider their views to inform the decision making process.

If the information relates to an ongoing criminal investigation or prosecution by any of the agencies then consultation must take place with the investigating officer and CPS as the matter will be *sub judice*. This will ensure that disclosure will not adversely prejudice the outcome of that matter.

Nothing in this section shall prevent individual Partner organisations from exercising their obligations and responsibilities under the FOIA or the EIR as they see fit.

10 Requests for Disclosure of Personal Information and Other Information Rights under the Data Protection Act 1998

Subject access requests and other notices relating to a data subjects rights made under the Data Protection Act 1998 will be co-ordinated and responded to by the organisation receiving the request and, where relevant, the fee. The charging of fees by Partners for subject access requests relating wholly or partly to data stored on Sentinel will be referred to the Strategic Information Management Group for consideration.

Organisations responding to such requests and notices should adopt the approach set out in section 9 above in doing so.

11 Joint Education

All users of the Sentinel system will be required to attend and satisfactorily complete an agreed training package covering both use of the system and information security issues. The training package will incorporate scenarios illustrating where sharing of information for the purposes of the Agreement is appropriate.

Users of the Sentinel system will be expected to familiarise themselves with the system operating procedures and the security operating procedures prior to attending the training.

The Group Security Steering Committee will identify the training needs of both new starters and refresher updates for existing users.

12 Information Quality

Standard information quality requirements are detailed in the Information Sharing Protocol.

Partners should take care when recording names, dates of birth and addressed to ensure that when data is shared it relates to the same person. Information quality is the responsibility of the IAO for the Partner entering the data.

13 Signatories

I, the undersigned, on behalf of my organisation, agree to the terms of the Sentinel Information Sharing Agreement.

Name – Sandra Whiles

Position – Chief Executive

Organisation – Blaby District Council

Signature Sandra Whiles .....

Date ..... 21/5/14 .....

Please retain the original and send a copy to

Michael Hopkins
Charnwood Borough Council
Southfield Road
Loughborough
Leicestershire
LE11 2TN

Appendix A – Data Protection Act compliance

The Data Protection Act 1998 requires that all processing of personal data must comply with the eight data protection principles. The following table sets out the principles and the steps that have been put in place to ensure that use of Sentinel complies with them.

Principle	Compliance Mechanism	Action Required by Partners
1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—	Section 2 of this Agreement sets out the legal basis for the information sharing. Fair processing information as described in paragraph 2(3) of Part 2 of Schedule 1 to the Data Protection Act must be provided to data subjects.	Ensure agreed fair processing information as described in paragraph 2(3) of Part 2 of Schedule 1 to the Data Protection Act is provided to data subjects, in particular when complainants make contact and when perpetrators are informed of disposals.
(a) at least one of the conditions in Schedule 2 is met, and	Use of Sentinel will involve the sharing of personal and sensitive personal information[1]. Each Partner can rely on paragraph 5(b) of Schedule 2 to the extent that they are performing their statutory functions and paragraph 5(d) of Schedule 2 to the extent that they are conducting any other functions of a public nature exercised in the public interest.	None. Further information relating to statutory powers can be found in section 2 of this Agreement.
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.	Use of Sentinel will involve the sharing of sensitive personal information. Each Partner can rely on paragraph 7(b) of Schedule 3 to the extent that they are performing their statutory functions. In addition, Leicestershire Police can rely on paragraphs 1 and 10 of the Schedule to SI 2000 No. 417[2]	None. Further information relating to statutory powers can be found in section 2 of this Agreement.

[1] Both personal data and sensitive personal data are defined in the Information Sharing Protocol.

[2] The Data Protection (Processing of Sensitive Personal Data) Order 2000. 1 The processing – a) is in the substantial public interest. (b) is necessary for the purposes if the prevention or detection of any unlawful act; and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes. 10 The Processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

Principle	Compliance Mechanism	Action Required by Partners
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	Section 3.8 of this Agreement sets out the further or secondary uses of the information held on the Sentinel system. Some of these uses require the consent of the data subject and others require disclosures to be recorded and reported to the Security & Change Management Control Group The Sentinel system includes functions which enable the use of the system to be audited. Auditing will be undertaken proactively to ensure that users do not undertake incompatible processing.	Ensure that a suitable description of Sentinel is included in notification to the Information Commissioner. Ensure compliance with reporting and auditing requirements.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	The data fields within the Sentinel system have been identified using the experience of operating Sentinel in Charnwood for a number of years. It has been agreed that a small number of super user/analysts at each local authority will be able to view records from outsider their authority's area so that issues of vulnerability can be identified. Use of this ability will be reviewed after 12 months to determine whether it is necessary.	The Sentinel Group Security Steering Committee and Security & Change Management Control Group are to review the use of the ad-hoc reporting function by super user/analysts after 12 months of operation of the system.
4. Personal data shall be accurate and, where necessary, kept up to date.	One of the main functions of Sentinel is to allow cases to be regularly updated. Section 12 of this Agreement sets out responsibilities for information quality.	Ensure Sentinel users update records, correct incorrect information and close cases in accordance with operating procedures and identify those records where the accuracy of the information is uncertain.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that	Section 3.7 of this Agreement sets out how long information will be kept for.	The Sentinel Group Security Steering Committee and Security & Change Management Control Group are to produce a Sentinel-

Principle	Compliance Mechanism	Action Required by Partners
purpose or those purposes.		specific retention policy after 12 months of operation of the system.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.	Section 10 of this Agreement sets out how subject access requests and other rights of data subjects will be dealt with.	None
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	Section 3.6 of this Agreement sets out how information security issues relating to the Sentinel system have been addressed. Appropriate agreements will be in place with third parties involved in the delivery of the Sentinel system.	These are set out in the Code of Connection and the Security Operating Procedures.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	This issue has been considered and there are no direct eighth principle issues to be addressed. Rackspace is an American-owned company and may be subject to requests for information under the U.S. Patriot Act but this is beyond the control of the Partners.	None

Appendix B - Data

The following table sets out a summary of the Sentinel data fields.

- Initial Contact Details – including name, address and contact details for complainant, whether the person is disabled, a repeat victim or vulnerable in some other way
- Incident Details – including the incident description and location, Home Office PEN Code, Police qualifier codes and a list of aggravating factors (age, alcohol, disability, domestic abuse, drugs, gender, race, religion, sexual orientation and student)
- People Involved – including their role in the incident (complainant, victim, witness, perpetrator and dependents of the same, address and contact details, age, gender, disability, vulnerability and any risk arising from a combination of personal protective characteristics and the circumstances of the incident, language, ethnicity and any support needs. Where the person role is that of complainant, victim or witness, details about any statements taken are also captured in this form. Where the person role is that of alleged perpetrator, then details of any ASB disposal/interventions are also captured here
- Task/Activity Alert – chronological list of activities performed in response to the complaint
- Case Working Sheet – supplementary information supporting the task alert list of activities
- Documents attached – could include statement of complaint, witness statement, copies of warning letters and court orders etc.

Where details of an incident which is an ASB crime are received by Leicestershire Police they will use their crime information system to record full details of the incident and its investigation. Leicestershire Police will add a skeleton record on Sentinel which refers to the fact that further information is recorded on their crime information system.

Where a complainant makes objections to information being shared and these concerns cannot be addressed, anonymised information relating to the incident will be recorded on Sentinel.

Access rights are not restricted on the basis of specific data fields (if a user has access to a record he/she has access to the whole record). However access is restricted geographically and the vast majority of local authority users will only have access to records which relate to incidents in the geographical area covered by their organisation (see section 3.5).

Location to which Sentinel record relates	Leicestershire Districts users	Districts Analyst/ super user	Leicester City Council users	City Council Analyst/ super user	Rutland County Council user	RCC Analyst/ super user	Leicestershire County Council user	LCC Analyst/ super user	Leicestershire Police user	Police Analyst/ super user
Leicestershire District	x (own district only)	x		x		x	x (all districts)	n/a	x	x
Leicester City		x	x	x		x		n/a	x	x
Rutland		x		x	x	x		n/a	x	x

Appendix C – Meetings

INFORMATION SHARING & EXCHANGE

Meeting Date:-

We, the undersigned, accept and understand the principles of the Sentinel Information Sharing Agreement.

We understand that the information that is shared and exchanged within the confines of this meeting is for the specific purpose of dealing with anti-social behaviour issues.

CONFIDENTIALITY GUIDANCE

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the Data Protection Act 1998, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Common Law Duty of Confidentiality, all attendees are asked to agree to the following. This agreement will be recorded in the minutes.

- Information may be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.

- A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the subjects' confidentiality and a breach of the confidentiality of the agencies involved.

- All documents exchanged should be marked 'Restricted – not to be disclosed without consent'. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.

- If further action is identified, the agency/ies that are involved with that action should retain possession of whatever information is required to assist them to proceed with the action(s) and should then make formal requests to or meet with any other agencies holding such personal information as may be required to progress the action quoting their legal basis for requesting such information outside of the meeting. No other party should use information exchanged during the course of this meeting.

- If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting and a decision will be made on the lawfulness of the disclosure. Such as the prevention or detection of crime, apprehension or

prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

ATTENDANCE LIST

SIGNATURE	**PRINT NAME**	ORGANISATION

Guidance for Chairs of Multi Agency Meetings

As the Chair of meetings at which personal/restricted information may be discussed you should ensure that the following takes place: -

That all people present are aware that any information shared at the meeting is to be held in confidence and only shared on a need to know basis. This could be done by reading out the confidentiality guidance or including the confidentiality guidance or reference to it as part of the attendance list.

You should consider who is present at the meeting and whether all those present will need to know about information which identifies individuals. If they do not, you should structure the meeting so that personal/restricted information is only shared after those who do not need to know have left the meeting.

Individuals who are present when personal/restricted information is being shared should be reminded that notes recording personal information should only be made when it is necessary for themselves or their organisation to carry out their statutory roles. Their notes should include the origin of the information so that the originating organisation can be consulted regarding any subsequent disclosure.

Any notes containing such information should be treated as ***'Restricted'*** and kept secure from unauthorised loss or disclosure, e.g. not lost on way back from meeting. If necessary to do so only emailed via 'gsi.', 'gcsx.' or 'pnn.', shredded securely etc.

That all documentation left by meeting attendees including notes/agenda/minutes of previous meetings and any other paperwork is removed from the room after the meeting and handled/destroyed in a manner appropriate to its content. Please bear in mind that leaving such information in a confidential waste bag leaves it available to anyone subsequently using the meeting room.

The minutes of the meeting which are circulated to all parties should not include personal /restricted identifiable information – particularly if these are to be published under your Freedom of Information Act publication scheme. You should also ensure that if the information in the minutes falls within the definition of 'restricted' below they should also be handled in a secure manner

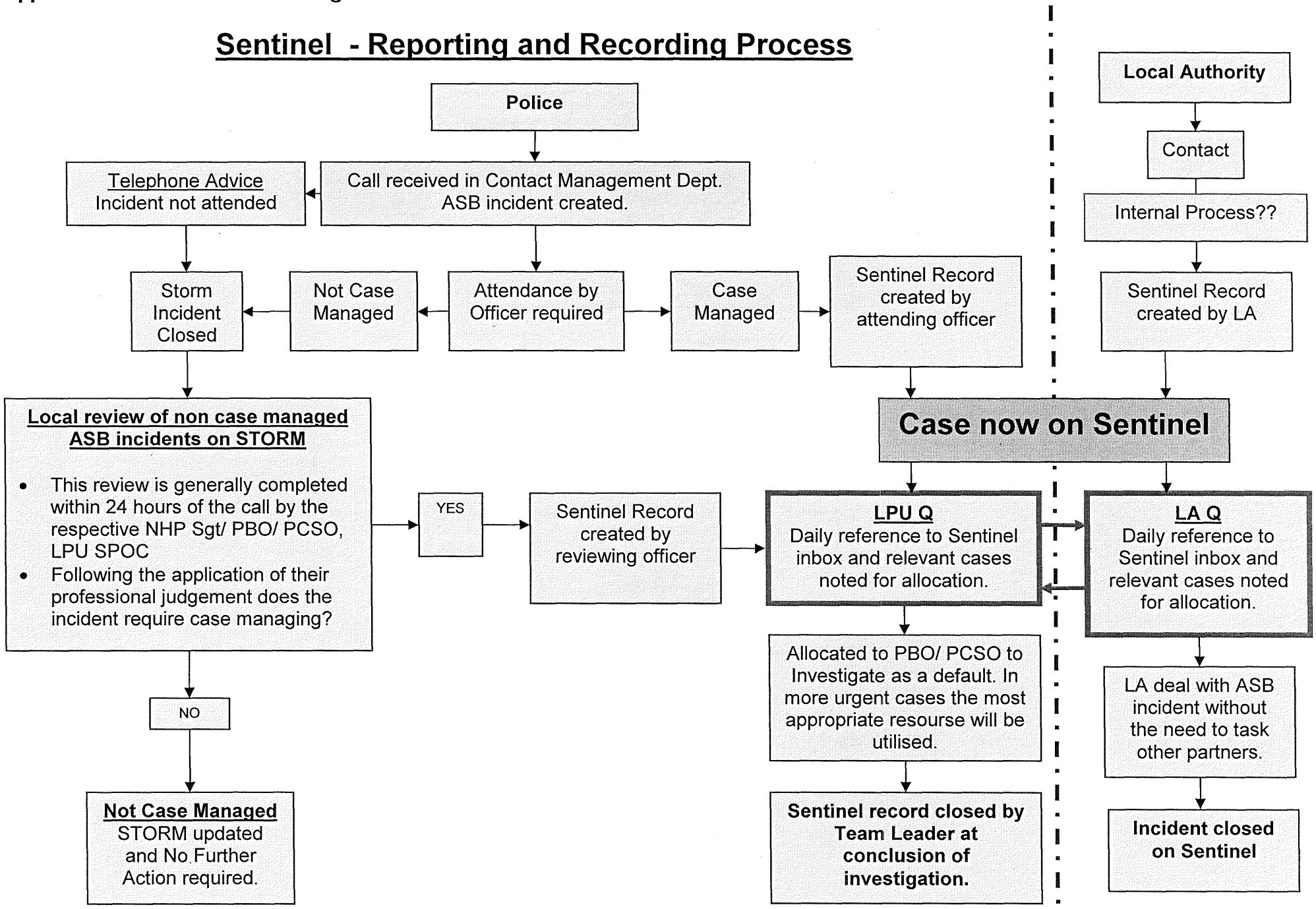
The relevant definition of 'Restricted' information:

If disclosure of the information would:

- cause substantial distress to individuals
- make it more difficult to maintain the security of the UK or allied forces
- prejudice the investigation or facilitate the commission of crime
- breach the confidence of material provided by third parties

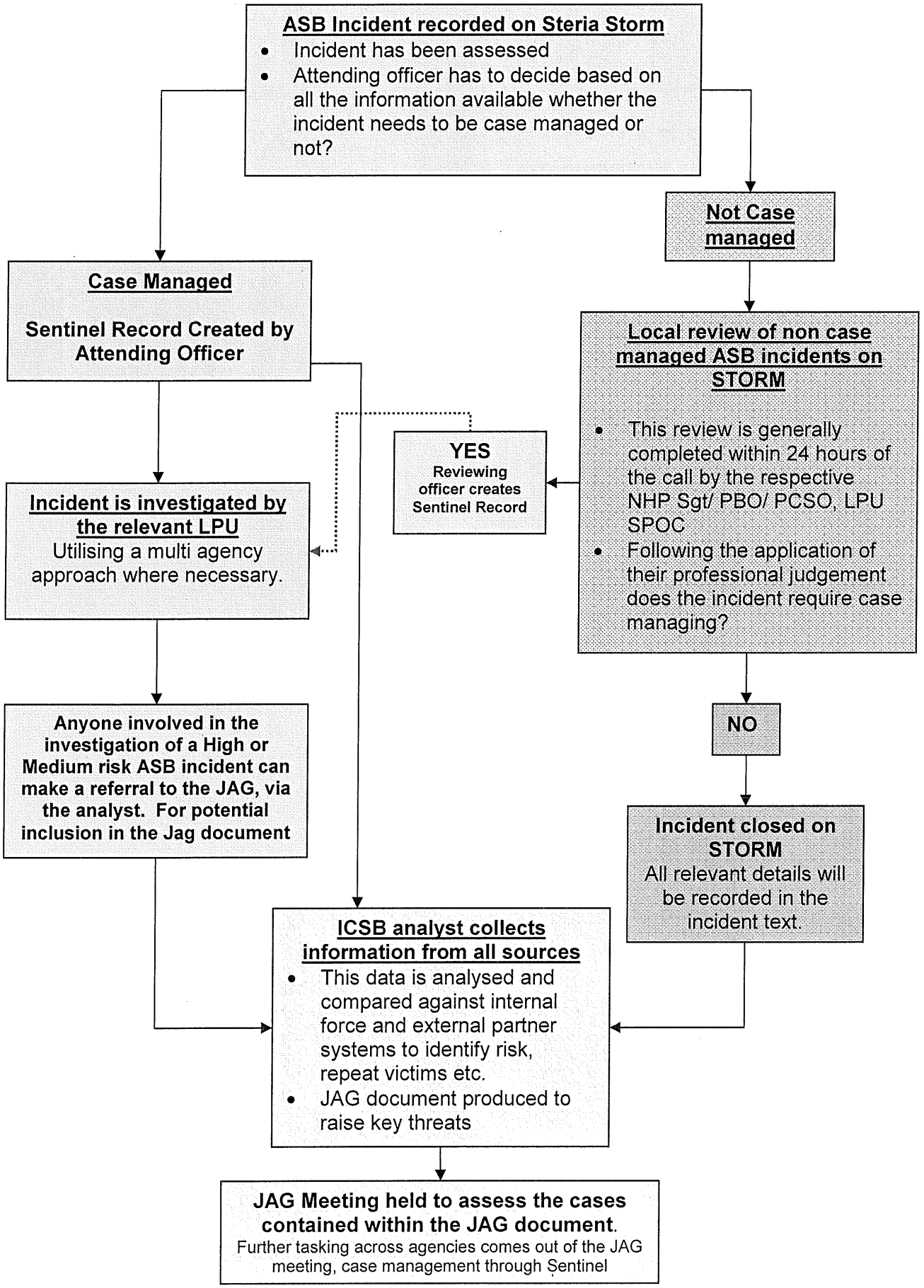
- breach statutory restrictions on disclosure of material (does not include the Data Protection Act 1998, where non-sensitive information is involved)
- undermine the proper management of the public sector and its operations

Appendix D – Information Sharing Processes



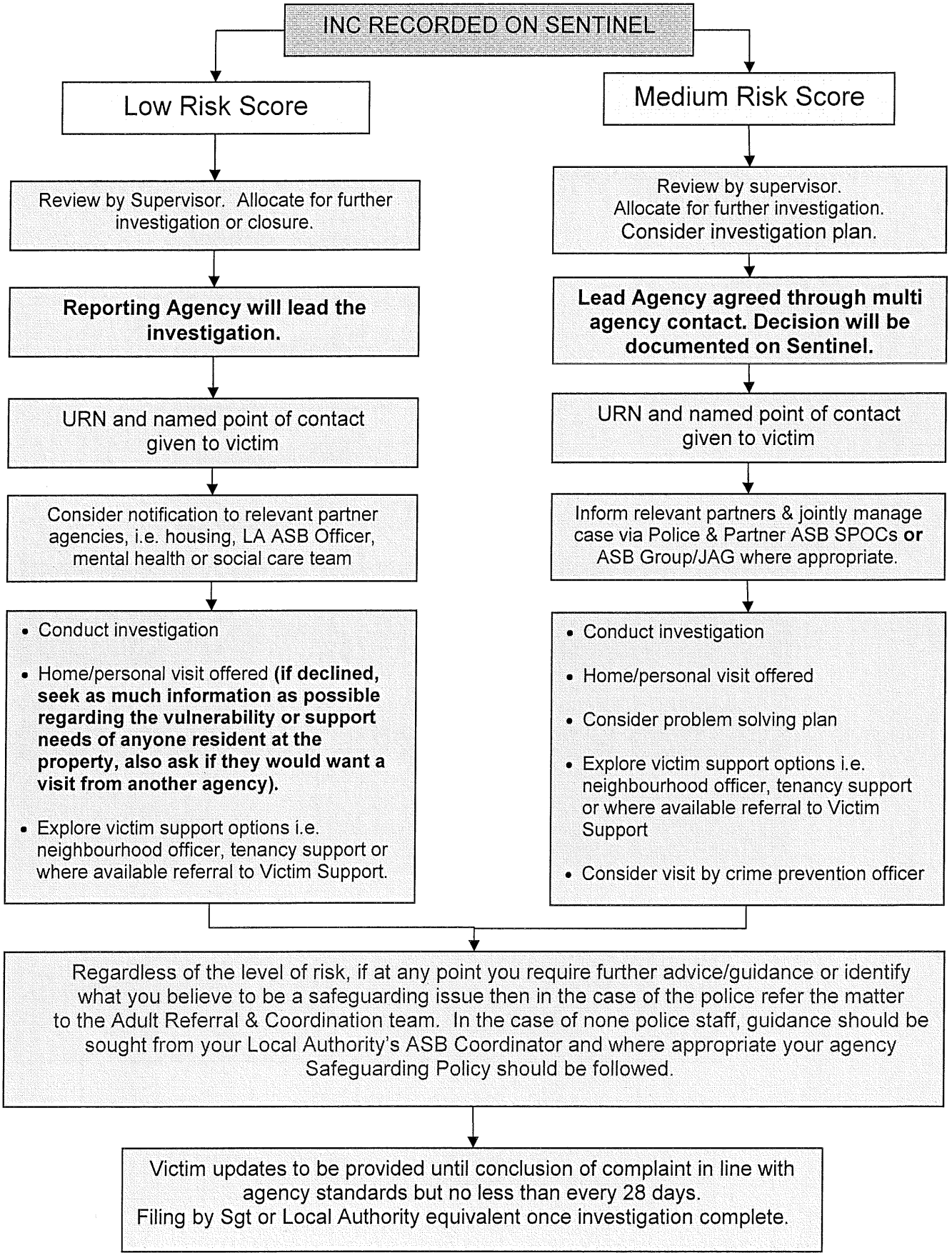
Appendix D – Information Sharing Processes

Information Management, Sharing and Oversight Process



Appendix D – Information Sharing Processes

Incident Management According to Risk



Appendix D – Information Sharing Processes