INFORMATION SHARING AGREEMENT to enable enforcement action and or compliance checks to be undertaken in relation licensed premises.

Partners to Agreement	
Leicestershire Police	The Police
Blaby District Council (BDC) Charnwood Borough Council (CBC) Harborough District Council (HDC) Hinckley & Bosworth Borough Council (HBBC) Leicester City Council (Licensing) (LCC) Leicester City Council Trading Standards (City TS) Leicestershire County Council Trading Standards (County TS) Melton Borough Council (MBC) North West Leicestershire District Council (NWLDC) Oadby and Wigston Borough Council (OWBC) Rutland County Council (RCC)	The Regulators

Date agreement comes into force:	21 February 2014

Date of Agreement Review:	Twelve months after date comes into force and five yearly thereafter

Agreement Owner:	Leicestershire Police

Protective Marking:	Not Protectively Marked

VERSION RECORD

Version No.	**Amendments Made**	**Authorisation**	**Date**
V1.0	ISA Template forwarded	Anne Chafer	
V1.1	Additional information added	Insp RIXON	20.08.2012
V1.2	Additional Information	Lee Mansfield	
V1.3	Legal Alterations	NW Leics Legal	
Final	Removed track changes	AM/AC	21 2 2014

1. PURPOSE

To document the process for the sharing of information between Leicestershire Police, County TS, BDC, CBC, HDC, HBBC, LCC, City TS, MBC, NWLDC, OWBC and RCC when personal information or sensitive personal information is required to enable the above named Regulators to consider appropriate enforcement action/compliance checks relating to premises which are licensed to sell alcohol. This is permitted under the following legislation; Licensing Act 2003 section 185.

2. OBJECTIVE

The Licensing Act 2003 section 185 specifically refers to information held by a "Responsible Authority" that can be disclosed to another responsible authority. The definition of a Responsible Authority is provided by Section 13(4) of the Licensing Act 2003. This includes the Chief Officer of Police. For the purposes of this Information Sharing Agreement (ISA) the following information will be shared:

The Regulators will share relevant personal and sensitive personal information from their data bases.

Types of information to be shared

- Names and address of licensed premises and individuals involved in the business
- Businesses who are about to be test purchased
- Businesses who have passed a test purchase operation
- Businesses who have sold an age restricted product to an underage person.
- A person who is to be issued with a Penalty Notice for Disorder (PND) because of an illegal sale of alcohol
- Businesses whose activities are causing concern in relation to the licensing objectives
- Demographic crime and anti social behaviour analysis, to identify problem areas and take positive action against those at risk of offending

Examples of information

- Complaints relating to off licences
- Proposed test purchase operations for off licence premises, subsequent outcomes of the operations and any enforcement action taken.
- Other information for the purposes of meeting the licensing objectives under the Licensing Act 2003

3. AREA OF RESPONSIBILITY

Off Licences – Trading Standards are primarily responsible for off licences in relation to underage sales for alcohol.
On Licences - The Regulators (except County TS) are primarily responsible for all licensing activities at On licence premises.

This Agreement will also apply to any exchange of personal or sensitive personal information which is intended to support action by Trading Standards at Off Licences or The Regulators at On Licences under any provision of the Crime & Disorder Act 1998 (as amended in 2000 & by the Police and Criminal Justice Act 2006); and any subsequent statutory amendment, addition or provision, which requires, or gives the power to exchange information.

4. POST HOLDERS RESPONSIBLE FOR DATA

This ISA has been developed to achieve the purposes/objectives as set out in Section 1. It is the intention that all aspects of information exchange and disclosure relating to this ISA shall comply with relevant legislation that protects personal data. The following table identifies posts and organisations responsible for this exchange for the purpose of this agreement.

POST	Organisation
Licensing Manager	Leicester Police
Licensing Assistants	Leicester Police
Licensing Sergeants	Leicester Police
Licensing Officers	Leicester Police
Operations Manager	Leicester Police
Trading Standards Officers	County TS
Environmental Services Team Leader	BDC
Technical Officer	BDC
Licensing Officers	CBC
Licensing Officers	HDC
Licensing Officers	HBBC
Licensing Officers	LCC
Licensing Officers	CITY TS
Licensing Officers	MBC
Environmental Health Manager	NWLDC
Licensing Team Leader & Officers	NWLDC
Licensing Officers	OWBC
Licensing Officers	RCC

5 CONSIDERATIONS BEFORE DISCLOSURE

The following should be considered prior to disclosure.

Ongoing Investigation

If the personal data relates to an ongoing investigation or prosecution by any of the Regulators then consultation must take place with the investigating officer and CPS (if applicable) **before any disclosure** to the Regulators as the matter will be sub judice. This will ensure that disclosure will not adversely prejudice the outcome of that matter.

Condition for Processing this Information

This information will be processed in accordance with Schedule 2, conditions 3 and 6 and Schedule 3, conditions 7 (1) (b) Data Protection Act 1998 and Statutory Instrument 2000 No 417 condition 10.

Public Interest

If informed consent has not been sought or sought and withheld the Regulators must consider if there is an overriding public interest of justification for the disclosure. The following questions should be considered to assist compliance with the Human Rights Act 1998.

- Is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the rights and freedoms of others?
- Is the disclosure necessary for the protection of young or other vulnerable people?
- Is the disclosure to enable the licensing objectives to be complied with?
- What will be the impact of the disclosure on the offender?
- Is the disclosure proportionate to the intended aim?

- Is there an equally effective but less intrusive alternative means of achieving that aim?

Proportionality

A key factor in deciding whether or not to disclose information is proportionality i.e. is the proposed disclosure a proportionate response to the need to protect the potential victim?
The amount of information disclosed and the number of people to whom it is disclosed should be no more than is necessary.

5 OWNERSHIP OF INFORMATION

The Chief Executive/Officer of the organisation which originally holds the information is the Data Controller. Once that information is shared with another partner to this ISA, the Data Controller of the organisation receiving the information becomes the Data Controller on receipt and will be responsible for ensuring that the information is held and used securely in accordance with this purpose, relevant legislation and this Information Sharing Agreement. Where a partner is using individuals employed by another agency to process the information, the partner will accept responsibility for this processing and ensure that appropriate signed contracts or agreements are in place to ensure that the conditions contained within this ISA are adhered to by these other agencies.

6 ACCESS RIGHTS

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult, the partners to this ISA will consult with the partner from whom the information originated and will consider their views to inform the decision making process.

7 EXCHANGE OF INFORMATION / DATA

Wherever possible, data will be used that will not directly identify individuals. However, the exchange of personal data will sometimes be required to achieve the purpose of this ISA.

Data which can be exchanged under this agreement can be divided into specific types:
If depersonalised information can be used to achieve the purpose, then there will be no data protection implications and the information can be disclosed freely.

Consideration should therefore be given to whether the purpose can be achieved using depersonalised information; or would failure to share personal information mean that the objectives of the ISA could not be achieved?

Personal Data
Personal data is information which relates to any living individual who can be identified from the data.

General Disclosure
To enable the requesting organisation to make the most informed, considered and effective decisions regarding the appropriate course of action in any specific case, data will need to be exchanged at the earliest possible opportunity.

Requests for personal or sensitive personal information must be in writing and should contain the following data, when relevant:

- The name of the individual about whom the data is requested and other identifying data available
- Specific details about what information is required
- The purpose for which the data is required
- The name and designation of the person requesting the data
- The secure e-mail address or fax number for responding to the request

The disclosure should be made in writing and retained along with the request for audit purposes.

The Police and Regulator in receipt of a request for personal data has the right to refuse to supply the personal data requested, but should record the reason for that decision.

8 SECURITY OF INFORMATION

Any Police information which you receive has a security marking of 'Restricted'. Appendix A specifies the security for processing this information[1]

Any information which relates to identifiable individuals or which may disclose current investigations or investigative techniques should be classified as "Restricted"

Restricted data will be sent by **secure** email between the Police and the Regulator using the PNN, CJSM or GCSX secure address conventions.

If information exchanged under this ISA is compromised this should be reported to the relevant Licensing Manager, who will in turn inform the Department within the Partner organisation dealing with Information Management so that appropriate action may be taken.

This may lead to disciplinary and/or criminal proceedings.

Faxing Good Practice

The following are considerations and good practice that should be followed when using fax.

1. *Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.*

2. *Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers* ***and*** *to send a 'Test Fax'.*

3. *Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.*

4. *If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.*

5. *Ring up or email to make sure the whole document has been received safely.*

[1] Processing is defined by the Data Protection Act 1998, but includes anything done with personal information including obtaining, reviewing, amending, updating, deleting etc.

6. *Use a cover sheet. This will let anyone know who the information is for and whether it is restricted or sensitive, without them having to look at the contents.*

9 REVIEW AND RETENTION OF INFORMATION

The storage of non personal and depersonalised data will be reviewed and out of date information will be permanently deleted.
Personal data should be retained in accordance with the partner's statutory requirements as documented in their retention policies. Data should only be retained for so long as is necessary.
The Police will retain information on the Licensing database "Inn Webb" and the Regulators will use the Premises database.

10 REVIEW OF THE ISA

This ISA will initially be reviewed after 12 months and then as necessary. If there are changes to this it will be reviewed and updated.

11 CLOSURE/TERMINATION OF THE AGREEMENT

Any partner organisation can immediately suspend or terminate this ISA. For this a suspension or termination notice should be in writing to the Licensing Manager.

12 FREEDOM OF INFORMATION ACT (2000) IN RELATION TO THIS AGREEMENT

Each Regulator shall publish this Agreement on its website and refer to it within its publication scheme. If a Regulator 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.

13 SIGNATORIES TO THIS AGREEMENT

I, the undersigned, on behalf of my organisation, agree to the terms of the Regulators ISA.

Name ..... Sandra Whiler .....

Position ..... Chief Executive .....

Organisation ... . Blaby District Council .....

Signature ..... Sandra Whiler .....

Date ..... 30/6/14 .....

Please retain the original and send an electronic copy to the
Information Manager,
Information Management Section,
Leicestershire Constabulary,
Force HQ,
St Johns,
Enderby,
Leicester LE19 2BX

A list of current signatories can be viewed on the Leicestershire Police website www.leics.police.uk

Appendix A:

Government Protective Marking Scheme
Handling Rules Regarding Information Marked or Classified as Restricted

Any information which relates to identifiable individuals or which may disclose current investigations or investigative techniques should be classified as "Restricted" and handled as instructed below.

Your Action	Security to be Applied
Storage of papers	Protected by one barrier, e.g. a locked container within a secure building/room
Disposal of papers	Use secure waste sacks. Keep secure when left unattended
Disposal of magnetic media	Securely destroy All types of discs – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction.
Movement within organisation via internal dispatch	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.
Movement between partner agencies	By post or courier in a sealed envelope. Do not show protective marking on the envelope
Organisation Data Network	May be used if network has been accredited to 'Restricted' or equivalent. Your IT dept should be able to advise
Email between partners	Only to emails using .PNN, .GCSX, .GSI, CJSM or .MOD secure addressing conventions. Remember emails to any other address are no more secure than writing the information on a postcard.
Removable media, USB, etc	Must be owned by the employer and encrypted with the encryption approved by the Force IT department. No personally owned removable media is to be used.
Internal and public telephone network	May be used.
Mobile telephone (voice and text)	Digital cell phones may be used. Only use analogue cell phones if operationally urgent, use guarded speech and keep conversation brief.
Radio not 'Airwave'	Radio networks are continually monitored. Care should be taken when disclosing information of a sensitive or personal nature and if not operationally urgent another means of communication must be sought.
Pager systems	Not to be used.
Fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.