

NORTH LANARKSHIRE COUNCIL

REPORT

To: ENVIRONMENTAL SERVICES COMMITTEE	Subject: INFORMATION SHARING PROTOCOL BETWEEN NORTH LANARKSHIRE COUNCIL AND POLICE SCOTLAND TO ASSIST WITH COLLABORATIVE WORKING ON A TRADING STANDARDS ATTACHMENT
From: HEAD OF PROTECTIVE SERVICES	
Date: 27 JANUARY 2015 Ref: CM/PB	

1. Purpose

- 1.1 To inform members of the decision to sign an information sharing protocol (ISP) between North Lanarkshire Council and Police Scotland, to assist with collaborative working on a Trading Standards attachment.

2. Background

- 2.1 North Lanarkshire Trading Standards and Police Scotland are committed to partnership working and continually look for opportunities to work together to detect, prevent and reduce crime, for the benefit of our local community.
- 2.2 Following discussions with officers at the Police Interventions Unit at Airdrie Police office, Trading Standards and Police Scotland have agreed to establish a three month pilot project during which a member of the Trading Standards Service will be embedded within the Lanarkshire Police Division. This project is intended to enable the parties as partners to liaise in enforcement work regarding the identification and disruption of criminal scams and rogue trading.
- 2.3 The attachment will operate on a three pronged basis, in respect of intellectual property crime (an area for which Trading Standards has a significant level of expertise and which is now a key performance indicator for Police Scotland), doorstep crime, and general intelligence liaison for the benefit of both agencies.
- 2.4 Trading Standards has been working closely with Police colleagues since the creation of Operation Doric in January 2013. This unit targets all forms of doorstep crime and collaborative working between Trading Standards and Police officers has demonstrated that by effective liaison the two enforcement agencies can achieve greater results.

3. Proposal

- 3.1 The purpose of the ISP is to clearly establish and set out the parameters under which the working practices of the two agencies are understood and the exchange of information during the pilot attachment is consistent with legislative requirements, in particular in terms of the Data Protection Act 1998. A copy of the ISP is attached as an Appendix to this report.
- 3.2 The attached Trading Standards staff member has been approved to Non-Police Personnel Vetting (NPPV) Level 2, will receive a data protection induction at the commencement of the pilot and will sign a confidentiality declaration.

- 3.3 The parties to the signed ISP will agree to share and exchange information as necessary, that is processed under the agreement (subject to the provisions of the Data Protection Act 1998) to work towards common aims to ensure positive outcomes. By targeting the perpetrators of crime and pursuing methods to tackle the criminal enterprises, we can create a fairer environment within which legitimate business has more chance to prosper. We can also serve the Community Plan aspiration to reduce the harm caused to our communities by organised crime.
- 3.4 All requests for data sharing between the partners to this ISP will be made in terms of agreed standardised forms and submitted in terms of section 29(3) of the Data Protection Act 1998. These enquiries will only be made for information which is specific to the common terms of the pilot Trading Standards attachment and will be securely stored. The information will not be retained by either party beyond their respective organisation's agreed retention and disposal policy.

4. Financial Implications

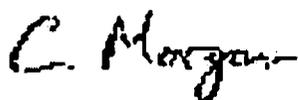
- 4.1 All related enforcement activities are contained within the Trading Standards budget and there are no additional financial implications arising from these proposals.

5. Corporate Considerations

- 5.1 This report has been agreed with colleagues in Democratic & Legal Services.

6. Recommendation

- 6.1 The Committee is invited to:
- (a) note the content of this report; and
 - (b) agree to homologate the decision to sign this ISP as agreed by the Executive Director of Regeneration & Environmental Services and the Convenor of the Environmental Services Committee.



CRAWFORD MORGAN
HEAD OF PROTECTIVE SERVICES

Local Government Access to Information Act: For further information please contact Paul Bannister, Business Manager, Trading Standards on 01236 856460.

INFORMATION SHARING PROTOCOL

INTRODUCTION

This Information Sharing Protocol (ISP) concerns the collaborative working arrangements between the Police Service of Scotland (Police Scotland) and North Lanarkshire Council (NLC).

Police Scotland and NLC are committed to partnership working and continually look for opportunities to work more closely with partner authorities and organisations to detect, prevent and reduce crime and ensure community and individual welfare and safety. The specific outcomes for the proposed short-term project are the:

- Prevention of/or detection of crime;
- Apprehension and prosecution of offenders;
- Identification and Disruption of criminal scams and rogue trading;

PURPOSE

The purpose of this document is to ensure effective co-operation between Police Scotland and NLC covering working practices and the exchange of information during the temporary attachment of a Trading Standards (TS) officer to Q Division (Lanarkshire). It will promote a clear understanding of the disclosure and transfer of information and the standards surrounding joint operations and investigations between the Partners.

This document seeks to support the exchange of information within legislative requirements and specifically in terms of the Data Protection Act 1998 (DPA) and Part 9 of the Enterprise Act 2002.

ROLES AND RESPONSIBILITIES

The Trading Standards departments' attached officer will be based in police premises and thus will require NPPV Level 2 vetting before beginning the secondment. The individual will also have to receive an induction into the information standards expected by Police Scotland and will sign the appropriate confidentiality declaration.

The attached officer will not have direct access to any Police Scotland information system or desktop/laptop; nor will police officers or staff have direct access to Trading Standards system or information. Despite this, there is an expectation that information from both will be shared verbally in the normal course of joint analysis around nominals, jobs of interest and shared operations. Any sharing of information will be in accordance with the procedures described below (section 4).

The attached officer will continue to work within his/her normal line management structure and employment policies, but will also report to Police Management as directed and determined by the project/operation being worked on. This direction will provide guidance to required Police policies and protocols. In addition, the Police Inspector with responsibility for the Divert/Deter portfolio will have overall responsibility for the attached officer during their time with Police Scotland. This will include all relevant Health and Safety requirements.

It is expected that the attached officer will work with a range of units; including, but not limited to, Interventions, Licensing and the Operation Doric team (doorstep crime).

An office base will be provided with access to telephony and copying facilities within Airdrie Police Office, however the attached officer will be required to work from different offices as determined by operations and with the individual's council management.

All officers sharing offices, or involved in joint operations, with the attached Trading Standard's officer will be reminded of their responsibilities in relation to Police information and security and the importance of confidentiality.

LEGISLATION AND POWER TO DISCLOSE INFORMATION

Each Partner shall have regard to their legal obligations and internal policy requirements for the proper handling of information, in particular policy requirements for the recording, retention and dissemination of information.

Relevant legislation for the purpose of this ISP includes (without limitation) the following:

- The Data Protection Act 1998 (DPA)
- The Human Rights Act 1998 (Article 8)
- The Police (Scotland) Act 1967
- The Enterprise Act 2002

The relevance of specific information will be determined (by the sharer) on its own merits, and where information is not relevant to the purpose for which it was requested, it will not be shared.

This agreement does not impose a duty to disclose information, nor does it provide the power to demand disclosure.

Partners will comply with the requirements below in respect of information disseminated between them.

REQUESTING AND SHARING INFORMATION

The specific legal gateway for requesting and sharing information is the appropriate section of Data Protection Act 1998 to the extent that non-disclosure of the requested information would be likely to prejudice one or more of those same purposes.

All decisions to share (or not to share) information will be made on a case-by-case basis, balancing the data protection and human rights of the individual against the policing purposes above. As such, the decision to share information must satisfy all of the following criteria:

- Information shared must be relevant, and necessary to achieve, or help to achieve, one or more of the purpose(s).
- All information shared must be proportionate to the purpose(s): it should be the minimum required to achieve the purpose(s) and not more.

Without limiting any right of Police Scotland to obtain a court order compelling the disclosure any information in its possession, the attached Trading Standards Officer will only be requested to assist Police Scotland under this ISP where non-disclosure would result in a substantial chance, not merely a risk, that the investigation, prosecution etc. would be prejudiced.

PROCESSES FOR REQUESTING INFORMATION

Police Scotland

The person submitting the request on behalf of Police Scotland should complete the standard DPA 29 request form clearly specifying the reasons for the request. Requests must be signed off at the rank of Police Inspector or equivalent.

In order that the information can be located, the request must contain sufficient detail:

- Name
- Date of birth
- Premises of interest
- Address

In the case of urgent enquiries, for example in cases of serious crime, and in particular where there is danger to life, the secondee will respond to the request at the earliest opportunity. *However*, requests must still be accompanied by the appropriate supporting DPA request form.

Trading Standards Officer

To request information from Police Scotland under this protocol the attached officer shall complete a written standard request (in the form set out in Appendix 1) clearly specifying the reasons why the exemptions to non-disclosure under the DPA apply.

Requests should be sent to the Police Scotland SPOC and will include:

- Name;
- Date of birth;
- Address;
- Nominal image, if available; and
- Checks already undertaken by the Trading Standards officer

Please note that where a Trading Standards investigation has uncovered evidence of criminal offences (outwith Trading Standards' remit) the Trading Standards Officer should refer the information to the Force SPOC and provide the following information:

A report of the investigation covering the details of offences and actions taken;

- Name of suspected offender; and
- Date of birth and address.

TYPES OF INFORMATION AND INTELLIGENCE TO BE SHARED

The information to be shared may include, but not exclusively, the following:

- Known business interests – to establish links between premises, other business activities, details of lock ups that may not be disclosed as business assets;
- Information regarding specific rogue trading companies – such as tarmac companies, roofers, builders, counterfeiters, scams, itinerant traders, door step crime.
- Such additional personal and sensitive personal data relating to any material health and safety or other significant public interest grounds; for example, it is known that a data subject carries weapons.

Partners may also provide depersonalised statistical information as they see fit in response to requests made by the other Partner.

Management of Information

All parties to the protocol agree to abide by the terms of the Data Protection Act 1998, in that:

- All data shall be securely transmitted and stored.
- All information provided shall be used for no other purposes than those contained within this protocol.

- Reasonable steps will be taken to ensure that all information disclosed is accurate.
- All information shall be updated as required.
- Information supplied by either agency party to this agreement will not be retained beyond the organisations agreed Retention and Disposal Policy

Protective Marking

The Police Service of Scotland uses the Government Protective Marking Scheme (GPMS) and information, which is shared, will carry a protective marking.

The protective markings used will be either **Restricted** or **Confidential**.

Restricted has the following meaning for the retention, transfer and disposal of information:

<i>Physical Security</i>
Restricted information should be protected by one security barrier; for example, a locked container, cupboard or filing cabinet.
<i>Transfer of Information</i>

<p>Hand delivery or post in a sealed envelope. The envelope should be addressed to a named person (addressee only) but must not bear the description RESTRICTED.</p> <p>E-mail can only be used if there is a secure network. In other words unless the e-mail address includes one of the following – pnn. gsi. or gcsx. - e-mail cannot be used.</p>
<p>Faxes MUST NOT be used.</p>

Confidential has the following meaning for the retention, transfer and disposal of information:

<i>Physical Security</i>
Confidential information in any format (and computers with access to confidential information) must be protected by TWO barriers; for example a locked container within a locked room.

Transfer of Information

By hand or by post in a double envelope with both envelopes fully addressed and marked for the addressee only. A return address will be given on the outer envelope. 'Confidential' will appear on the internal envelope only.

E-mail **MUST NOT** be used.

Disposal

A cross cut shredder must be used for paper, which will then be put in confidential sacks. These sacks should not be left unattended.

Magnetic data/information should be overwritten with an approved software utility. Floppy disks should be dismantled, cut into four and disposed off with normal waste.

Breaches of Security

All known or suspected breaches of security in relation to terminals and any information shared under this agreement - such as misuse or abuse of the system, misuse or abuse of information shared, unauthorised processing of data, unauthorised disclosure of information, malicious software attack, denial of service attack - are to be reported to the respective organisation's Information Security Officer, Data Protection Officer or equivalent. Once notified of a breach of security an investigation will take place to identify, where possible, who carried out the breach, what information has been compromised, whether the integrity of the system has been compromised etc.

Where any breach of security may amount to criminal activity, this must be reported to the Police Service of Scotland, which will investigate the matter and, where appropriate, report the circumstances to the Procurator Fiscal.

Where relevant or necessary, partner organisations are to be informed of any breach and provided with sufficient details to enable them to retain assurance in the confidentiality, integrity and availability of the information and the processes supporting information exchange, and to undertake their own risk assessments.

Access to Information

Access to information compiled as part of any of these processes is available either under subject access rights, as described in the Data Protection Act 1998 (Section 7), or the Freedom of Information (Scotland) Act 2002 (FOI). Where access is requested advice must be sought from the organisation's Freedom of Information or Data Protection Officer.

Where a request has been received and the partner holds any information that originated from the other partner or where the partner is considering the disclosure of information that may impact on a criminal investigation or the provision of a service, it is essential that the originator of the information is consulted prior to any disclosure. The ultimate decision as to whether to disclose the information lies with the organisation that received the request; however, the originator of the information should be given the opportunity to ensure that FOI (or Data Protection) exemptions are suitably applied.

Complaints from data subjects, or their representatives, about information held by the partnership will be investigated first by the organisation receiving the complaint, although action that affects any of the signatories will not be taken without the consent of all relevant parties.

Review

This protocol will be reviewed at the end of the three month trial attachment period.

Signatures

By signing this Protocol, the 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 its purposes.

Signatories must also ensure that their organisation complies with all relevant legislation.

Signed on behalf of The Chief Constable of the Police Service of Scotland:

.....
Rank/Position:
Date:

Signed on behalf of North Lanarkshire Council

.....
Title:
Rank/Position:
Date:

APPENDIX 1 REQUESTS FOR PERSONAL DATA

REGIONAL OFFICE ADDRESS

Dear

REQUEST FOR PERSONAL DATA UNDER SECTION 29(3), THE DATA PROTECTION ACT 1998

I am making enquiries into [details]:

NAME:

DATE OF BIRTH:

ADDRESS:

These enquiries concern:

- a) the prevention or detection of crime
- b) the apprehension or prosecution of offenders
- c) *Explanation of a specific crime/offence if necessary*

I confirm that the personal data requested is required for one or more of these purposes and failure to provide the information will, in my view, be likely to prejudice these purposes. Notwithstanding the foregoing, it is required to assist the Intelligence Unit of TSS assess the physical risk to Trading Standards staff carrying statutory enquiries.

I should be grateful if you would let me have the following information under Section 29(3) of the Data Protection Act 1998:

I confirm that the personal data requested is required for the above purpose and failure to provide information will, in my view, be likely to prejudice that purpose.

Signed..... Grade.....

Name..... Date.....

NB: - The pro-forma needs to be countersigned.

Countersigned..... Grade.....

Name..... Date.....