

INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**



PURPOSE	The purpose of this Information Sharing Agreement is to facilitate the lawful exchange of data in order to comply with the statutory duty on Chief Police Officers and relevant agencies to work together for the purpose of implementing strategies and tactics in relation to crime reduction and the prevention and detection of crime throughout England, Wales and Northern Ireland.
PARTNERS	The National Policing Lead for Hate Crime on behalf of The Police Service of England, Wales and Northern Ireland (Hereafter referred to as 'The Police') Stop Hate UK
Endorsing Forces	This agreement is in force for all police areas and allows for all forces to use this agreement to share included information with named partners. It does not need to be individually endorsed but any force may agree additional local data sharing agreements not included in this agreement by adding agreed additions to the document, countersigning it and sharing a copy with the other parties.
DATE OF IMPLEMENTATION	1 st March 2018
REVIEW DATE	Next Review due April 2019
Original signed copy held at	PSNI Headquarters

Version No.	Date	Amendments made	Authorised by
1.0	9.4.18	N/A	ACC Hamilton (PSNI)



Contents

Protective Marking:

NOT PROTECTIVELY MARKED

Disclosable under FOIA 2000

YES

Enquiries to:

paulx.giannasi@gmp.police.uk

Police Organisation

The National Police Chief's
Council

Date Last Reviewed

9.4.18

Next Review Date

1.4.19

Introduction	4
1.Purpose	4
2.Partners	5
3.Powers	5
4.Force Level Information Shared	5
5.National Level Information Shared	6
6.Use of shared information	6
7.Stop Hate UK Information Shared	7
8.Process	7
9.Policies and Procedures	8
10.Data Retention	8
11.Disclaimer	8
12.Indemnities	8
13.Single Point of Contact (SPoC)	8
14.Signatures	9
1.INFORMATION MANAGEMENT REVIEW	10
APPENDIX A – Designated Authorised Staff	11



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**



1. INTRODUCTION

- 1.1. This agreement has been developed to facilitate partnership working between police forces in the UK - hereafter referred to as The Police and the identified partner agency - Stop Hate UK. This agreement identifies the legal powers and methods of sharing information in order to achieve common goals for the benefit of our community.
- 1.2. The Police are committed to partnership working, and continually look for opportunities to work more closely with identified partners to detect, prevent and reduce crime.
- 1.3. In adopting this partnership approach it is important that the policies/practices of the agencies involved compliment each other to ensure that any action taken is appropriate, necessary, proportionate and consistently applied.
- 1.4. This agreement outlines the need for the police and the agency involved to work together to alleviate crime in England, Wales and Northern Ireland and provides a framework for action.

2. PURPOSE

- 2.1. To provide Stop Hate UK with up-to-date information relating to incidents which involve members of the affected communities. This will better prepare Stop Hate UK to protect victims and other sections of our community and to provide advice which will help citizens to protect themselves and their communities.
- 2.2. It is also anticipated that this disclosure will assist in improving public confidence in The Police and relationships between The Police, victims and the community as a whole.
- 2.3. The Crime and Disorder Act 1998 and the Police Reform Act 2002 places obligations on various agencies as defined in the legislation to co-operate in the development and implementation of a strategy for addressing the issues relating to crime and disorder in their area. Effective information exchange is the key to partnership working.
- 2.4. The effectiveness of information exchange is a reflection of the effectiveness of the partnership as a whole.
- 2.5. The protocol is designed to:
 - Support action in accordance with any of the legislative provisions of the Crime and Disorder Act 1998 and Data Protection Act 1998 where personal data is included,
 - Govern the use and management of information provided by the parties to this agreement,
 - Assist with the exchange of information to support other crime reduction activities,
 - Document the specific purposes for which the signatory partners have agreed to share information,



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

- Describe the roles and structures that will support the exchange of information between partners,
- Set out the legal gateway through which the information is shared, including any reference to the Data Protection Act 1998 (DPA), General Data Protection Regulation (GDPR) [when in force], the Human Rights Act 1998 (HRA) and the Common Law duty of confidentiality,
- Describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities included under the DPA and any partner specific security requirements,
- Ensure compliance with individual partners policies, legal duties and obligations,
- Ensure that the police comply with the Code of Practice on the Management of Police information made under the Police Act 1996 and the Police Act 1997, and
- Ensure that the police comply with the information Commissioners Code of Practice on Data Sharing.
- Ensure that the police comply with the Code of Ethics as outlined by the College of Policing in accordance with the purpose of this agreement.

3.PARTNERS

- 3.1. This agreement is between the following partners:
- 3.2. ACC Mark Hamilton on behalf of all Chief Officers of England, Wales and Northern Ireland (The National Policing Lead);
- 3.3. Rose Simkins, Chief Executive of Stop Hate UK

4.POWERS

- 4.1. This agreement fulfils the requirements of the following legislation:
 - The Civil Evidence Act 1995
 - The Crime and Disorder Act 1998
 - The Police Reform Act 2002
 - The Rehabilitation of Offenders Act 1974
 - The Human Rights Act 1998 (article 8)
 - The Data Protection Act 1998 (sections 29[3]) & 35[2])
 - Corresponding and relevant legislation and policies in Northern Ireland
 - Code of Practice on the Management of Police information made under the Police Act 1996 and the Police Act 1997



5.FORCE LEVEL INFORMATION SHARED

- 5.1. The Police agree to share the following information at force level:
- Anonymised details of incidents/crimes relating to, or believed to be targeted at our communities.
 - Anonymised details of any arrests made in relation to these incidents.
- 5.2. The information will be disclosed in any of the following methods as agreed between Stop Hate UK and local police body:
- The referral of individual victims and witnesses who has expressly agreed that their information shall be passed to Stop Hate UK for victim support purposes.
 - A 'Stop Hate UK Return' from the police, either 'as required' when relevant information or incidents have occurred or at regular intervals agreed by partners. This may contain a summary of local intelligence relevant to Stop Hate UK and their community and the local implications of national and international events.
 - Regular meetings to compare anonymised data to identify crime trends, to inform crime reduction activity and to evaluate the effectiveness of crime reporting structures. The duration of regular meetings to be agreed with each force.
 - Ad-hoc meetings to be arranged at times of specific need due to, for example, increased community tension or increased levels of hate crime reporting.
- 5.3. It is envisaged that there may be rare occasions where personal or sensitive personal information may need to be disclosed to Stop Hate UK for a valid policing purpose. These disclosures operate outside of this agreement and an appropriate officer must assess any potential disclosure as relevant and proportionate on a case-by-case basis.
- 5.4. In order to facilitate this agreement individual police agencies should nominate a Single Point of Contact (SPoC) to oversee data exchange processes either personally or by nominated deputies under the oversight of the SPoC.
- 5.5. Any information routinely disclosed by The Police will be wholly anonymised by the relevant Police SPoC prior to disclosure. No information classed as personal by virtue of the Data Protection Act 1998 will be routinely disclosed under this agreement.

6.NATIONAL LEVEL INFORMATION SHARED

- 6.1. The National assessment of UK Hate Crime data is the responsibility of the National Community Tension Team (NCTT) and on behalf of the National Policing Lead for Hate Crime the NCTT will share the following information at a National level:



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

- The NCTT will produce 6 monthly data assessments in relation to hate crimes across the UK. This assessment will be briefed to Stop Hate UK in an agreed meeting format.
 - In exceptional times of heightened tensions within our communities, the information provided by forces to the NCTT may be shared in an anonymised format. Force returns will be utilised to provide trend analysis of hate crime reporting across the UK. Comparative data from previous reporting periods may be used to establish increases or decreases in reporting levels.
 - All ad hoc requests for National data or information must be directed to the NCTT via email on: NCTT.nctphq@met.pnn.police.uk where each request will be assessed for proportionality and feasibility by the Head of NCTT in conjunction with Senior Officers relevant to the subject of the request.
- 6.2. The NCTT in their capacity as national lead for community tension monitoring in the UK will disseminate the weekly Partners Element (Not Protectively Marked) document to Stop Hate UK.
- 6.3. In respect of the No Hate Speech UK project, the police will share information of trends of hostility that have been detected or reported in online hate. Such information will not include personalised information of individual victims (without the explicit consent of the victim) and will not target known 'real named' perpetrators, although it may include sites where hostility is prevalent, target groups and accounts used to target individuals or groups for hate material that could be illegal if the poster and jurisdiction was known to be in the the United Kingdom but where there identity of the poster can not be demanded from the host.
- 6.4. The National Policing lead, as the representative of all forces, may authorise the sharing of any anonymised data originating from forces for the benefit of The Police in delivering its services.

7.USE OF SHARED INFORMATION

- 7.1. The information shall be exclusively used for the following purposes:
- To provide Stop Hate UK with relevant information relating to incidents which involve members of the UK community. This will better prepare Stop Hate UK to protect their members and other sections of the community and to provide advice which will help citizens to protect themselves and their communities.
- 7.2. This information is for the purposes outlined in this agreement and should not be shared with a third party without the consent from the originating author.
- 7.3. It is recognised that the purpose, outlined above, may require access to data previously 'protectively marked' by a Chief Constable under the Government Protective Marking Scheme

8.STOP HATE UK INFORMATION SHARED



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

- 8.1. Stop Hate UK may share concerns and issues with The Police. It is not envisaged that they will share personal data as part of this data sharing agreement. Incidents or crimes will be reported through normal reporting channels.
- 8.2. Stop Hate UK will share anonymised crime and incident data to identify crime trends, to inform crime reduction activity and to evaluate the effectiveness of crime reporting structures.
- 8.3. Regular meetings to be agreed with each force or national unit, dependent on requirements.
- 8.4. Ad-hoc meetings to be arranged at times of increased community tension within the UK Community or areas impacting the UK communities.
- 8.5. The No Hate Speech UK project will use the information about online hate to brief participants in order to;
 - 8.5.1. Support targeted victims of online hate
 - 8.5.2. Report harmful or illegal hate material to the hosts or relevant agency under the sole direction and discretion of the Stop Hate UK management
 - 8.5.3. Directly challenge untruthful and damaging material to provide and accurate counter-narrative to online hate material in support of the duties of the Equalities Act 2010 and to reduce the harm caused to communities.

9.PROCESS

- 9.1. It is not envisaged that there will be many bespoke requests made outside of the agreed periodic reports. Bespoke requests will be dealt with by the SPoC and this information sharing agreement will be used as a guide.
- 9.2. The information identified above will be disclosed via a format deemed most appropriate by the SPoC given the circumstances of the request.
- 9.3. Where regular (e.g. daily, weekly, monthly) requests for information are processed within the terms of the agreement, it is the responsibility of the SPoC to keep a log of the dates, reasons for disclosure, data sent and the requestor.
- 9.4. Any requests for personal information outside of this agreement must be made in writing. Requests for personal information will be reviewed on a case by case basis and must comply with the Data Protection Act principles found in the ISA Guidance Notes.
- 9.5. Requests may be made by secure e-mail addresses. Any message containing personal information should not be sent via non-secure email. The circulation of police information must follow the guidance laid down in the Government Protective Marking policy.
- 9.6. Requests for information may be made by telephone in cases of emergency. (For example, where there is a risk of immediate violence). Where this occurs, the request for information must be recorded and submitted retrospectively.
- 9.7. Regular audits of the information exchanged should be undertaken by the SPoC to ensure that they contain details of the decisions made and that these decisions to share information have been made in accordance with the agreement, the Data Protection principles and for a legitimate policing purpose. (As defined in the code of practice for the Management of Police Information).



10.POLICIES AND PROCEDURES

- 10.1. All policies and procedures outlined in the Appendices to this agreement shall be complied with to ensure adherence to all rules on information Security and Management are upheld.
- 10.2. Procedures may be altered on written agreement of the SPoCs and will form part of an Appendix to this agreement.
- 10.3. All information sharing agreements shall be reviewed by the Information Management department who will identify whether the completion of a full or small Privacy Impact Assessment (PIA) is required.
- 10.4. No information provided under this agreement shall be disclosed to a 3rd party without the explicit consent of the data controller. Requests must be made in writing to the appropriate police SPoC (originating force or national unit).
- 10.5. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
- 10.6. Partners will respond to any notice from the data owner that imposes requirements to cease or change the way in which data is processed.
- 10.7. Each Partner Data Controller is responsible for responding appropriately to Subject Access Requests addressed to them and to providing information to the data subject to enable them to make appropriate requests to other Partners where appropriate.
- 10.8. Data subjects have the right to object to processing. How the data subject makes such objections should be detailed in each Partners Privacy Notice. It is the responsibility of each partner to produce and maintain their own Privacy Notice.

11.DATA RETENTION

- 11.1. Any information held by the Partner Agency will be disposed of, in line with its protective marking, or returned to The Police, at the request of The Police.

12.DISCLAIMER

- 12.1. The information Provider (Data Controller) disclaims all liability to the data recipient in connection with the data recipients use of data supplied under this agreement and shall not, under any circumstances, be responsible for any special, indirect or consequential loss or damages including but not limited to loss of profits arising from the use of the data by the data recipient.
- 12.2. Information shared by The Police may include intelligence which may not have been corroborated but all other detail will be relevant and believed accurate at the time of obtaining it until proven otherwise. Any false allegation will still be retained as an accurate record of fact.

13.INDEMNITIES



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

13.1. The data recipient shall indemnify the Information Provider in full in respect of any loss or damage caused to the information Provider as a consequence of the unauthorised disclosure of data supplied under this agreement.

14. SINGLE POINT OF CONTACT (SPOC)

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

14.2. The specific responsibilities of the SPoC are:

- Ensure compliance with the policies and procedures outlined in the appendices to this agreement,
- Ensure that the information exchanged is kept secure and confidentiality is maintained as appropriate to the information's level of protective marking as defined by the Data Controller,
- Deciding on a case by case basis if and why a public interest overrides a duty of confidence,
- Ensuring any changes to the SPoC are confirmed in writing,
- Ensuring that professional, ethical standards are maintained as outlined in the Code of Ethics,
- Ensuring that the Data Protection Principles are upheld,
- Providing appropriate staff training on this agreement, and
- Provide adequate arrangements to test adherence to the agreement.

15. SIGNATURES

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

15.2. It is the responsibility of forces that use this agreement to appoint appropriate SPoCS to manage the performance of this agreement.

1. Signatory for The Police:

Name: Mark Hamilton

Position: Assistant Chief Constable PSNI and National Policing Lead for Hate Crime

Signed:



Date: 9.4.2018



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

2. Authorised Signatory for Stop Hate UK:

Name: Original signed by Rose Simkins

Position Chief Executive Officer

Date 9.4.2018

3. Authorised Signatory for [Specify force]

Name:

Position:

Signed:

Date

1. INFORMATION MANAGEMENT REVIEW

(Internal use only)

- 1.1. This agreement has been submitted to the Information Management Department at Nottinghamshire Police for review and the following checks have been completed:

	Yes	No	N/A
Privacy Impact Assessment required?			
Privacy Impact Assessment completed?			
Privacy Law/Data Protection Compliance Check required?			
Privacy Law/Data Protection Compliance Check completed?			

APPENDIX A – DESIGNATED AUTHORISED STAFF

Confidentiality Agreement

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

DESIGNATED AUTHORISED STAFF FOR

[Insert force area]

Name	Contact Details	Signature
------	-----------------	-----------



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

	Organisation Role E-mail: Tel:	
	Organisation Role E-mail: Tel:	
	Organisation Role E-mail: Tel:	
	Organisation Role E-mail: Tel:	
	Organisation Role E-mail: Tel:	
	Organisation Role E-mail: Tel:	

Please continue on another sheet if necessary.

Designated Authorised Staff/ Management Co-ordination

The SPoC will be responsible for providing their own force Information Manager with the contact details of the 'Designated Authorised Staff'. Designated Authorised Staff will be those who, after being subject to any vetting requirements, will have access to the information shared under this agreement. A list of Designated Authorised Staff will be made available within these documents. Failure to adhere to this may result in a temporary suspension of information sharing with the Police.

The information exchanged will only be used for the purpose for which it has been provided and it will be securely stored and returned to the Police when no longer required or destroyed at their request.

Notification of Moves and Changes of Staff

The SPoC will be responsible for maintaining the list of 'Designated Authorised Staff' ensuring that it is current and that any required amendments are completed. A new and revised list of Designated Authorised Staff will be submitted to the relevant Police force every six months via the Information Manager so that the Force may update their records of staff with access information under this agreement. The new document will include the signatures of the Designated Authorised Staff named within it.

Vetting



INFORMATION SHARING AGREEMENT

This document is **NOT PROTECTIVELY MARKED**

Non-Police Personnel Vetting relates to the vetting of persons other than police personnel, who require access to police premises or police information systems. They include, for example, Language Service Providers, Crime & Disorder partners, HM Customs & Excise, Department of Works & Pensions, Work Experience, Lay Visitors and a variety of contractors and volunteers, some of whom require full access to our IT systems or to sensitive police information. The purpose of vetting is to provide a standard level of protection of both government and police assets.

All non-police personnel requiring such access will be required to submit a personal information document giving consent for the vetting checks to be undertaken by the Vetting Unit. The individual will be checked on the information supplied against the following databases:

Criminal Records (spent convictions are to be included)

Police Intelligence

Special Branch

Professional Standards

National Government (where applicable)

Financial (where applicable)

