Title of Report:	**MOU AND INFORMATION SHARING AGREEMENT WITH PSNI REGARDING THE HEALTH PROTECTION (CORONAVIRUS RESTRICTIONS) REGULATIONS (NORTHERN IRELAND) 2020 AS AMENDED**
Committee Report Submitted To:	**ENVIRONMENTAL SERVICES COMMITTEE**
Date of Meeting:	**9th June 2020**
For Decision or For Information	**FOR DECISION**

Linkage to Council Strategy (2019-23)	
Strategic Theme	Resilient Engaged and Healthy Communities
Outcome	Implementation of statutory requirements
Lead Officer	Head of Health & Built Environment

Budgetary Considerations	
Cost of Proposal	N/A
Included in Current Year Estimates	N/A
Capital/Revenue	N/A
Code	N/A
Staffing Costs	N/A

Screening Requirements	Required for new or revised Policies, Plans, Strategies or Service Delivery Proposals		
Section 75 Screening	Screening Completed:	~~Yes/No~~ N/A	Date:
	EQIA Required and Completed:	~~Yes/No~~ N/A	Date:
Rural Needs Assessment (RNA)	Screening Completed	~~Yes/No~~ N/A	Date:
	RNA Required and Completed:	~~Yes/No~~ N/A	Date:
Data Protection Impact Assessment (DPIA)	Screening Completed:	~~Yes/No~~ N/A	Date:
	DPIA Required and Completed:	~~Yes/No~~ N/A	Date:

1.0 Purpose

The purpose of this report is to consider and agree a Memorandum of Understanding (MOU) and Information Sharing Agreement (ISA) with PSNI regarding the enforcement of the Health Protection (Coronavirus Restrictions) Regulations (Northern Ireland) 2020.

2.0 Background

The above regulation were made on the 28th March 2020 by the Department of Health in response to the coronavirus disease (COVID-19) pandemic. The PSNI were the only body designated to enforce the Regulations until their amendment on the 15th May 2020, (see previous report item).

EHNI under the direction of SOLACE NI and in conjunction with the Department of Health and PSNI have been working to produce guidance for Council officers on the division of enforcement responsibilities and the exchange of information to ensure effective and consistent enforcement and line with Councils own enforcement policies.

The purpose of the MOU is to:

1. Establish an agreed framework between the Council and the PSNI regarding enforcement of the 2020 Regulations;

2. Clarify the general roles and responsibilities of each Party in relation to regulation 3 (requirement to close premises and businesses during the emergency) and regulation 4 (further restrictions and closures during the emergency period);

3. Set out in general terms the specific types of enforcement activity that each Party has responsibility for under the 2020 Regulations.

4. Set out in general terms the basis of an information sharing protocol between the parties for the purposes of enforcement under the 2020 Regulations; and

5. Set out the review, dispute and termination arrangements.

The draft MOU may be found at Appendix 1 to this report.

The purpose of the ISA is to:

1. This agreement is designed to facilitate the legitimate, timely and secure sharing of information between the Councils and PSNI, in order to enable the effective administration and enforcement of the Regulations.

2. Such information may include personal data and this ISA is designed to ensure that the handling of all personal data is in accordance with the relevant data protection requirements.

3. This ISA supplements those policies in order to enable the sharing of information between the parties to the ISA in order to enforce the Regulations.

The draft ISA may be found at Appendix 2 to this report.

3.0 Recommendation

It is recommended that Council that council agree to signing the final versions of each document to ensure consistent and efficient enforcement of the Regulations. It is further recommended that authority be given to the Director of Environmental Services to sign on behalf of Council.

MEMORANDUM OF UNDERSTANDING BETWEEN CAUSEWAY COAST AND GLENS BOROUGH COUNCIL AND THE POLICE SERVICE OF NORTHERN IRELAND

TO SET OUT THE ENFORCEMENT RESPONSIBILITIES UNDER THE HEALTH PROTECTION (CORONAVIRUS, RESTRICTIONS) REGULATIONS (NORTHERN IRELAND) 2020 AS AMENDED AND REPORTING ARRANGEMENTS

Scope

1. This Memorandum of Understanding (MOU) is between Belfast City Council and the Police Service of Northern Ireland with regard to the enforcement of regulation 3 (requirement to close premises and businesses during the emergency) and regulation 4 (further restrictions and closures during the emergency period) of the Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2020 as amended to protect public health.

Definitions in this MOU

2. "2020 Regulations" means the Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2020 as amended.

   "the Council" means Causeway Coast and Glens Borough Council.

   "Licensed premises" means those premises which sell alcohol, amusement arcades, bingo halls and any other licensed premises in respect of which PSNI are the normal enforcing authority.

   "Parties" means the Council and the Police Service of Northern Ireland and any party may be construed in the singular.

"PSNI" means the Police Service of Northern Ireland.

Purpose

3. The purpose of the MOU is to:

- Establish an agreed framework between the Council and the PSNI regarding enforcement of the 2020 Regulations;
- Clarify the general roles and responsibilities of each Party in relation to regulation 3 (requirement to close premises and businesses during the emergency) and regulation 4 (further restrictions and closures during the emergency period);
- Set out in general terms the specific types of enforcement activity that each Party has responsibility for under the 2020 Regulations.
- Set out in general terms the basis of an information sharing protocol between the parties for the purposes of enforcement under the 2020 Regulations; and
- Set out the review, dispute and termination arrangements.

4. When the content of the MOU is agreed a Council representative and a PSNI representative shall be co-signatories of this MOU. It shall come into effect from the latest date of signing by the Parties. This MOU will remain in force indefinitely unless superseded by another MOU or equivalent document.

5. The Parties enter into this MOU independently and nothing herein shall be construed as establishing a partnership or joint venture between the Parties, nor may either Party profess to represent the other Party, save with written consent in advance from the other Party.

Roles and responsibilities

6. The Council and the PSNI are committed to working together to protect public health.

7. While the general responsibilities of each Party to this agreement are outlined below, there may be occasions when it would be appropriate for the parties to be involved in the same investigation. This shall primarily be determined by the nature of the business however, any decision on which Party may take the lead role shall be determined by mutual agreement at the time.

Councils Responsibilities pursuant to this MoU

8. The Council will be responsible for enforcing any requirement or restriction imposed by regulation 3 (requirement to close premises and businesses during the emergency) or regulation 4 (further restrictions and closures during the emergency period) of the 2020 Regulations in relation to all non-licensed premises within the Council's area.

9. The Council will refer all complaints regarding regulations 3 and 4 of the 2020 Regulations, in licensed premises, to the PSNI.

PSNI Responsibilities pursuant to this MoU

10. PSNI will be responsible for enforcing any requirement or restriction imposed by regulation 3 (requirement to close premises and businesses during the emergency) or regulation 4 (further restrictions and closures during the emergency period) of the 2020 Regulations in relation to all Licensed Premises..

11. The PSNI will continue to deal with all complaints made to it in relation to all alleged breaches of the Regulations which were notified to it prior to 25th May 2020 including, for the avoidance of doubt, complaints pursuant to regulations 3 and 4.

12. The PSNI will refer all subsequent complaints regarding regulations 3 and 4 of the 2020 Regulations, in non-licensed premises, to the Council.

13. The PSNI has sole enforcement responsibility under Regulation 5 (restrictions of movement) and Regulation 6 (restrictions on gatherings) of the 2020 Regulations.

14. Depending on the individual circumstances of an investigation, PSNI support may be requested by the Council (e.g. where a breach of the peace is reasonably anticipated or where the entry to premises is being made under warrant). PSNI will use all reasonable endeavours to support the Council when required subject to the availability of police resources.

Information Sharing Protocol

15. An Information Sharing Protocol (ISP) shall be developed to assist the sharing of information for purposes of enforcement under the 2020 Regulations. Any ISP will be subject to the agreement of both Parties.

Notification of complaints

16. Any complaints which are received by a Party which appears to be the responsibility of the other Party to this MoU shall refer that complaint to that Party within 12 hours on a working day (Monday to Friday), or at the commencement of the next available working day where that is not feasible.

17. The Council will refer all complaints which appear to be the responsibility of PSNI to a Single Point of Contact where they will be triaged and allocated to the relevant district for action as outlined in Appendix 1.

18. The PSNI will refer all complaints which appears to the responsibility of the Council to the Council. The relevant contact officers are outlined in Appendix 1.

19. If a complaint relates to social distancing issues within premises which are permitted to be open, this is a health and safety issue which falls under the Health and Safety at Work (NI) Order 1978. This Order is enforced by both the Health and Safety Executive for Northern Ireland and the District Councils. If the premises relates to; construction, manufacturing, heavy industry, transport, government property,

agriculture, educational, nursing homes and hospitals, the complaints should be referred to the Health and Safety Executive for NI, for investigation. Complaints relating to all other types of premises should be referred to the Council in which the premises are situated for investigation. See Appendix 1 for contact details.

20. To facilitate the monitoring of complaints incidents generally, the Council and the PSNI will log all complaints and the number of ongoing and completed investigations or prosecutions.

Legal Status

21. While this MOU constitutes a statement of mutual intent between the Council and PSNI, it does not constitute a legally binding obligation. While each Party has specific responsibilities arising from this MOU, it creates no rights in favour of any Party.

Review Arrangements

22. This MOU will be reviewed each time the 2020 Regulations are reviewed, every 21 days from 18th April 2020. However, either Party may seek a review of this MOU by request in writing to the other Parties. Where a meeting is considered necessary, the hosting and location of such meeting shall be determined at the time by mutual agreement between the Parties. This will be referred to the Strategic Coordination Centre (SCC).

23. This MOU may also be revised by either Party by written communication between the Parties however, no revision shall take place without the agreement of the other Party. Written notification of any revision from one Party shall be considered by the other Parties within 1 month of notification. A determination of acceptance or rejection of such revisions by the other Parties shall be made and issued to the Parties within that 1-month period.

24. Where both Parties agree to any revision, whether by meeting or in writing, the Council shall be responsible for making such revisions and recirculating the revised MOU, or appending any revisions to the MOU, to the other Party.

Dispute Resolution

25. A dispute shall be deemed to have arisen when either Party notifies the other Party in writing to that effect.

26. The Parties shall use all reasonable efforts to resolve any dispute that may arise under this MOU through good faith negotiations. Each Party shall nominate a senior representative of its management to meet with the SCC at any mutually agreed location to resolve the dispute.

27. If a resolution cannot be reached the matter will be referred to SOLACE and INSERT PSNI DETAILS.

Termination of Agreement

28. This MOU may be terminated by either Party, and such termination must be in writing to the other Party and give at least 1 month's notice of termination.

29. Such termination shall not detract from any statutory responsibility for enforcement of the 2020 Regulations by the Council or PSNI.

Confidentiality

30. Each Party shall observe confidentiality in relation to shared information which is not already in the public domain.

31. Each Party shall ensure that the information it supplies to the other Party is subject to appropriate safeguards in order to avoid prejudicing the interests of all parties. Both Parties accept that in certain circumstances a duty of confidence may arise and that shall respect legal requirements of confidentiality.

32. It is for the Party providing the information to state what, if any, restrictions there should be upon its use. Each recipient Party shall treat the information it receives in accordance with the restrictions which are specified as to its use.

33. Disclosure of information shall be subject to the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

34. Some information will be subject to statutory or other restrictions, such as the Data Protection Act 2018, The General Data Protection Regulations or the Official Secrets Act 1989, or protecting commercial or other interests, which may mean that there will be restrictions on the category of persons who may have access to the material. Such access shall be determined by the supplier of the information (i.e. the Councils or the PSNI) and the recipient Parties must adhere to any such restriction.

Operational Arrangements

35. Operational arrangements will be kept under review by the Council and PSNI, and may be subject to change. The Council and PSNI will liaise with one another and provide mutual support as the need arises. Contact details are contained in Appendix 2.

Media Queries

36. Where either Party received a media query which relates to enforcement responsibilities of more than one Party any response must be agreed by both Parties to which the query relates prior to issue wherever possible.

Appendix 1

Contact Details for complaints referral to Councils

Council	Email address/telephone number
Belfast City Council	envhealth@belfastcity.gov.uk
Lisburn and Castlereagh District Council	ehealth@lisburncastlereagh.gov.uk
Ards & North Down Borough Council	Covid19Enquiries@ardsandnorthdown.gov.uk 0300 013 3333
Mid & East Antrim Borough Council	mea.envhealth@midandeastantrim.gov.uk
Causeway Coast & Glens Borough Council	healthandsafety@causewaycoastandglens.gov.uk 028 2766 0257
Antrim & Newtownabbey Borough Council	envhealth@antrimandnewtownabbey.gov.uk 028 90340160
Armagh City, Banbridge and Craigavon Borough Council	ehealth@armaghbanbridgecraigavon.gov.uk 0300 0300900
Newry, Mourne & Down District Council	ehealth@nmandd.org 03301374024
Fermanagh and Omagh District Council	eh@fermanaghomagh.com
Derry City & Strabane District Council	healthandsafety@derrystrabane.com, 02871253253
Mid Ulster District Council	environmentalhealth@midulstercouncil.org 03000 132 132

Emails will only be responded to during office hours, Monday to Friday, 9am to 5pm.

Contact Details for complaints referral to PSNI

Central database details:

Contact Details for complaints referral Health and Safety Executive for NI

Email: mail@hseni.gov.uk or telephone: 0800 0320 121.

Appendix 2

Council Contact details for liaison/operational issues

Council	Lead Officer details	Deputy Officer details
Belfast City Council	Mark McGovern 07713684708 mcgovernm@belfastcity.gov.uk	Carole Ann McCrory 07875015145 mccroryc@belfastcity.gov.uk
Lisburn and Castlereagh District Council	Richard Harvey 07739948570 richard.harvey@lisburncastlereagh.gov.uk	Gareth Lennox 07739948571 Gareth.lennox@lisburncastle
Ards & North Down Borough Council	Marcus Potts marcus.potts@ardsandnorthdown.gov.uk 07734580480	Hazel McKee hazel.mckee@ardsandnortho 07464654233
Mid & East Antrim Borough Council	Elaine Thompson elaine.thompson@midandeastantrim.gov.uk 02825633130	Elise Logan elise.logan@midandeastantr 02825633131
Causeway Coast & Glens Borough Council	Bryan Edgar Bryan.Edgar@causewaycoastandglens.gov.uk 07809552931	Sharon McClements, Sharon.McClements@cause 07490565523 Amber Holmes Amber.Holmes@causewayc 07711087772
Antrim & Newtownabbey Borough Council	Colin Kelly colin.kelly@antrimandnewtownabbey.gov.uk	Karen Allen karen.allen@antrimandnewto Julie Neill julie.neill@antrimandnewtow
Armagh City, Banbridge and	Elizabeth Reaney elizabeth.reaney@armaghbanbridgecraigavon.gov.uk	. Peter Girvan peter.girvan@armaghbanbri

Craigavon Borough Council	0300 0300900 Mobile 07799471156	0300 0300900 2. Claire Dawson claire.dawson@armaghbanb 0300 0300900
Newry, Mourne & Down District Council	Aoibheann McLernon aoibheann.mclernon@nmandd.org 0330 137 4000	Eoin Devlin Eoin.Devlin@nmandd.org 0330 137 4000
Fermanagh and Omagh District Council	Gerry Tierney gerry.tierney@fermanaghomagh.com	Aisling Shortt aisling.shortt@fermanaghom
Derry City & Strabane District Council	Barry Doherty barry.doherty@derrystrabane.com 07713068552	Paul Rafferty paul.rafferty@derrystrabane. 07739882420
Mid Ulster District Council	Fiona McClements fiona.mcclements@midulstercouncil.org 07748148703	Melanie Patterson melanie.patterson@midulste 07766740916

Police

PSNI Contact details for liaison/operational issues

Council area	**PSNI Lead Officer details**	**PSNI Deputy Officer details**
Belfast City Council		
Lisburn and Castlereagh District Council		
Ards & North Down		

Borough Council		
Mid & East Antrim Borough Council		
Causeway Coast & Glens Borough Council		
Antrim & Newtownabbey Borough Council		
Armagh City, Banbridge and Craigavon Borough Council		
Newry, Mourne & Down District Council		
Fermanagh and Omagh District Council		
Derry City & Strabane District Council		
Mid Ulster District Council		

Signed on behalf of

Council: _____

Name: _____

Grade: _____

Position: _____

Date: _____

Signed on behalf of

The Police Service of Northern Ireland_____

Name: _____

Rank: _____

Position:_____

Date: _____

Coronavirus Restrictions
Information Sharing Agreement

An agreement between District Councils and the Police Service of Northern Ireland to facilitate the effective enforcement of The Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2020, through the legitimate, timely and secure sharing of information

Version:	0.1
Status:	Draft
Date of issue:	26 May 2020

Document Ref:	[insert reference]

Purpose:	The purpose of this agreement is to formalise information sharing arrangements between the eleven District Councils and the Police Service of Northern Ireland enable the legitimate, timely and secure sharing of information to facilitate the effective enforcement of The Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2020, as amended.

Partners:	District Councils and the Police Service for Northern Ireland

Date Agreement comes into force:	[Day] [Month] 2020

Date for Review of Agreement:	[Day] [Month] 2020

Agreement drawn up by:	Causeway Coast and Glens Borough Council

Location of the Original Agreement:	

Document history and version control

Version	Description / amendments	Authorisation	Date of issue
0.1	1st Draft		26 May 2020

Index

1. Introduction

1. The partners to this Information Sharing Agreement ("ISA") are the District Councils in Northern Ireland ("the Councils"), listed in Appendix 1 (each a "Partner Council"), and the Police Service of Northern Ireland ("PSNI").

2. This ISA has been developed using guidance from the Data Sharing Code of Practice published by the Information Commissioner's Office ("ICO"), currently under review.

3. The lead body for the development, implementation and review of this ISA is Environmental Health Northern Ireland ("EHNI").

4. EHNI is a Heads of Service advisory group of the Society of Local Authority Chief Executives in Northern Ireland ("SOLACE NI").

5. The Chair EHNI has a co-ordinating role with the Councils for matters relating to this ISA and all work arising from it.

6. Once the content of this agreement has been agreed and is deemed acceptable by all parties, the Chair EHNI will sign this agreement on behalf of the the eleven district councils together with the [insert Rank / Title of appropriate PSNI Officer], who will sign it on behalf of PSNI.

2. Background

1. The Councils have been designated under The Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2020, as amended ("the Regulations") to enforce the legal requirements in respect of businesses that must remain closed (Regulation 3) and those businesses which can function subject to certain restrictions (Regulation 4).

2. The Regulations have been introduced in response to the serious and imminent threat to public health which is posed by the incidence and spread of severe acute respiratory syndrome coronavirus 2 (SARSCoV-2) in Northern Ireland.

3. The Councils will deal with enforcement of the Regulations in relation to requirements placed on businesses only (Regulations 3 and 4)

4. Under regulation 7 of the Regulations the Councils have been designated by the Department of Health as having powers of enforcement including the service of fixed penalty notices on persons committing an offence and the instigation of legal proceedings.

5. PSNI will continue to deal with enforcement of the Regulations in relation to individuals, gatherings and non-business premises and venues.

6. It has been agreed by the Councils and PSNI that PSNI will also continue to deal with enforcement of Regulations 3 and 4, as they relate to certain types of premises, detailed in Appendix 2, including those, such as public houses, which are licensed for the sale of alcohol.

7. There is, therefore, a shared responsibility for enforcement of the Regulations between the Councils and PSNI.

8. The effective enforcement of the Regulations will, therefore, necessitate close cooperation and the sharing of information between the Councils themselves and between the Councils and PSNI, in the interests of protecting public health.

9. The need for the sharing of such information may arise in a number of ways, including:

- A Council or PSNI may receive a complaint or enquiry, in error, which is the responsibility of another Partner council or PSNI, necessitating the sharing of that information.

- Council officers may need to request police support when enforcing the Regulations at certain premises, necessitating once again the sharing of information in advance of carrying out visits to those premises.

- Some duty holders will also conduct their business at premises in multiple Council areas and as fixed penalty amounts increase with the number of fixed penalty notices issued against an individual, information on persons who have been issued with a fixed penalty may need to be shared.

10. Failure to share necessary information would result in an increased risk to public health.

11. As such information may contain personal data, such as names and contact details of complainants, the sharing process is governed by legislation which must be adhered to in all cases.

3. Purpose of the Agreement

1. This agreement is designed to facilitate the legitimate, timely and secure sharing of information between the Councils and PSNI, in order to enable the effective administration and enforcement of the Regulations.

2. Each of the Councils and PSNI are committed to working together and when necessary and appropriate, sharing information that will protect public health.

3. Such information may include personal data and this ISA is designed to ensure that the handling of all personal data is in accordance with the relevant data protection requirements.

4. PSNI and each of the Councils have their own data protection policies for handling personal data inside their respective organisations, which will continue to apply.

5. This ISA supplements those policies in order to enable the sharing of information between the parties to the ISA in order to enforce the Regulations.

4. Lawful Basis for Data Sharing

1. In the United Kingdom, the processing of personal data is governed by:

    - The Data Protection Act 2018 (“DPA”); and
    - The General Data Protection Regulations (“GDPR”).

2. Before sharing any personal information, at least one lawful basis for processing must be identified from a number of provisions. These bases are defined within the above legislation:

    - GDPR (supplemented by Part 2 of DPA) covers the processing of personal information for all non-law enforcement purposes.
    - DPA (Part 3) covers those provisions that relate to the processing of personal data for law enforcement reasons.

    Lawful basis for data sharing under this agreement

3. Part 3 of DPA sets out a separate data protection regime for authorities with law enforcement functions when they are processing personal data for law enforcement purposes.

4. The law enforcement purposes are defined under section 31 of DPA as: “The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”

5. As the primary purpose of sharing personal data under this ISA is law enforcement, Part 3 of DPA provides both PSNI and the Councils with the lawful basis for data sharing.

6. Using this lawful basis necessitates that PSNI and Councils comply with the six law enforcement data protection principles detailed in Appendix 3 of this ISA.

7. It will be the responsibility of the parties to the ISA, when personal data is being shared, to ensure there is full compliance with the legal principles set out in the GDPR and DPA, the Human Rights Act 1998 and the Common Law Duty of Confidentiality insofar as they apply to the information sharing taking place under the terms of this agreement.

8. Seven Golden Rules for Information Sharing are listed in Appendix 4 to this ISA.

9. Public interest considerations when sharing information are listed in Appendix 5 to this ISA.

10. The Councils and PSNI must decide whether or not they can or should share information and decisions should be made on a case-by-case basis, using professional judgement taking account of the matters set out in Appendix 3, Appendix 4 and Appendix 5.

11. Managerial or legal advice should be sought where necessary.

5. Data that may be Shared

1. The Council and PSNI must only share information that is relevant and proportionate, based on the merits of each case.

2. Information will only be used for the purpose for which it was requested and will not be shared with any other party.

3. The following examples of data that may be relevant to enforcement of the Regulations and may be shared, should be used as a non-exhaustive guideline:

    - Incident details
    - Witness statements
    - Photographs / visual images
    - Enforcement action taken under the Regulations against an individual
    - Correspondence from enquirers and complainants
    - Information received by one partner that must be passed to another partner for information and/or investigation

6. Security, Data Handling and Management

1. Personal data and special category personal data must not be emailed over the open internet without encryption or secure email.

2. It is critical that a record of the exact information shared **must be** retained by the provider and recipient organisations, i.e. the PSNI or the relevant Partner Council must record the specific information released by whom, to whom and when. This is to ensure the integrity and continuity of any information that maybe used for evidential purposes and this record provides an accurate audit trail in the event of either the PSNI or a Partner Council being challenged. It also provides provenance with regard to the sequence of its formal ownership, custody, storage and sharing. There can be no compromise on this obligation and failure to properly record the process will dilute and weaken the agreement. All Partner Councils and the PSNI must open a file for the sharing of information in respect of this agreement.

3. The primary method of requesting information from PSNI will be completed by e-mail via the following email addresses:

   xxxxx@psni.pnn.police.uk

   xxxxx@psni.pnn.police.uk

   The Councils will receive information in written format until secure email addresses can be obtained.

4. The Data Protection legislation requires that personal data is:

   Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5. In addition, each organisation must ensure that measures are in place to do everything reasonable to:

   - Make accidental compromise or damage unlikely during transmission by using secure email, storage, handling, use or processing;
   - Deter deliberate compromise;
   - Promote discretion in order to avoid unauthorised access;
   - Information must only be accessed for legitimate purposes in a manner consistent with investigation and enforcement priorities and only where there is a “need to know”.

6. The Councils remain the owner (data controller) of any personal information provided to the PSNI and the PSNI remains the owner (data controller) of any personal information it provides to the Council.

7. Both the Councils and PSNI must hold the personal information provided by either party in strictest confidence and must not disclose it to any third party without the prior written consent of either party.

8. Both the Councils and PSNI must ensure that only those of its employees, who require access for lawful business purposes, will be able to view and process the data. All staff will have received appropriate training in data protection awareness to enable them to understand their responsibilities under GDPR and DPA to maintain the security and confidentiality of personal information.

9. No processing will be performed by a sub-contracting organisation without the knowledge and agreement of the parties involved.

10. Guidance on handling of PSNI data is attached as Appendix 6

Please note: Faxing is NOT a secure means of transmission for information relating to investigations or enforcement under the Regulations and should NOT be used.

7. Subject Access (SAR), Freedom of Information (FOIA) & Environmental Information Regulations (EIR)

1. The Councils and PSNI must have their own information governance protocols and guidelines and these should also be adhered to for the purposes of investigation and enforcement under the Regulations.

2. These will include how to process requests for information under the DPA, Freedom of Information Act 2000 ("FOIA") or the Environmental Information Regulations 2004 ("EIR"). These must be dealt with by the party who receives the request unless they do not hold the information requested.

3. Where information held is relevant to the request and is identified as having originated from the PSNI, another Council or organisation, it will be the responsibility of the receiving party to contact the originator of the data to determine whether the originator wishes to claim an exemption under the provisions of either the DPA, FOIA or EIR. The receiving party should be mindful that they must respond to requests within 28 calendar days under the DPA and 20 working days under the FOIA and EIR.

4. The responsibility to deal with a request for personal data, general information or environmental information will rest with the agency who receives it. Information must not be disclosed to any other person without prior consideration from the originating sources.

8. Breaches

1. A breach of the proper handling of personal data may seriously undermine and affect the credibility of the sharing of information for investigations and enforcement under the Regulations. It may also be a breach of the DPA and may attract enforcement action by the ICO.

2. The Councils and PSNI will ensure that staff are aware they may be subject to disciplinary action and/or legal proceedings if they unlawfully or without appropriate authority disclose personal data on a basis that cannot be justified on legal grounds.

3. If it is believed that information supplied by an organisation has been lost or inadvertently disclosed, a data loss/incident response plan must be engaged. The Councils or PSNI upon discovering any breach of the Data Protection legislation involving information shared must inform the relevant party to this agreement and provide full and comprehensive details of the breach.

4. All organisations must ensure they are familiar with the ICO guidance on data security breach management and its guidance on how and when to notify the ICO in the event of a breach.

5. Whoever is responsible for the breach may be accountable and ultimately subject to any potential enforcement action recommended by the ICO after an investigation.

9. Training

1. The Councils and PSNI will ensure that members of their staff who are involved in sharing information will have received adequate information and training in relation to their responsibilities and obligations imposed by this ISA.

10. Complaints regarding Information Sharing

1. Complaints related to the processes and procedures (information sharing) should be submitted in writing by the complainant.

2. If the complaint relates to the procedure listed within this ISA, then whoever receives the complaint must immediately bring this to the attention of the Chair EHNI.

3. Chair EHNI will acknowledge the complaint and convene an immediate meeting of those involved to agree on how best to proceed. Chair EHNI must respond within 20 working days of receipt, where possible.

4. Should the complaint be against a specific Partner Council, as opposed to the actual sharing of information, the initial complaint should be sent directly to the designated officer for that Council and dealt with via that Council's complaints procedure.

11. Retention and Review

1. The information processed in relation to investigations and enforcement under the Regulations will be retained in line with the PSNI and each Partner Council's retention and disposal schedule.

2. The information Sharing Agreement will be reviewed by the Chair EHNI after 3 months. The ISA may be reviewed sooner should there be changes to legislation or other exceptional circumstances. All changes to the ISA are to be agreed and approved by all parties to the agreement prior to the changes taking place.

12. Withdrawals

1. The designated officer for any Partner Council who wishes to withdraw from this ISA must inform Chair EHNI in writing. Chair EHNI will inform the relevant Council liaison officers and the PSNI in writing.

2. Information processed by the leaving Partner Council, which is no longer relevant should be destroyed in accordance with the respective Partner Council's guidelines.

13. Agreement

This Agreement is made on [insert date] between PSNI the Partner Councils listed in Appendix 1.

We the undersigned agree that we will:

- Be bound by the terms of this agreement ;
- Use the information only for the purposes stated;
- Keep the data for no longer than is necessary;
- Provide access to the minimum number of people for fulfilling the purpose;
- Maintain a current list of those with access to the information;

Each party to this agreement will not pass on or disclose any of the information provided to them to any Third Party unless required to by law.

Material changes to the agreement may be made only with the consent of all parties.

Signed on behalf of the PSNI	**Signed on behalf of Councils**
Department:_____	Organisation*: SOLACE? Or individual councils*
Name: _____	*Name*:
Grade/Title: _____	*Position/Title*:
Date: _____	*Date*: _____

Appendix 1

Partner Councils

The following Councils are a party to this agreement:

- Antrim and Newtownabbey Borough Council
- Ards and North Down Borough Council
- Armagh City, Banbridge and Craigavon Borough Council
- Belfast City Council
- Causeway Coast and Glens Borough Council
- Derry City and Strabane District Council
- Fermanagh and Omagh District Council
- Lisburn and Castlereagh City Council
- Mid and East Antrim Borough Council
- Mid Ulster District Council
- Newry, Mourne and Down District Council

Appendix 2

PSNI enforcement responsibilities in relation to Regulations 3 and 4

PSNI will maintain responsibility for the investigations and enforcement under the Regulations in relation to the following types of premises:

[insert list of premises that PSNI have agreed to regulate, e.g. licensed premises, bingo halls, etc.]

Appendix 3

The Law Enforcement Data Protection Principles

1. Processing of personal data for any of the law enforcement purposes must be lawful and fair.

2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;

   Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

3. Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and; Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

5. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

6. Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Appendix 4

Seven Golden Rules for Information Sharing

1. **Remember that the Data Protection legislation is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) form the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being:** Base your information sharing decisions on the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared accurately.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix 5

Public interest considerations when sharing information

The following points must be considered before sharing information:

- The right to confidentiality and the public interest in upholding this right;
- Proportionate Response;
- Respective risks to those affected;
- Passing need;
- Need to know of other agencies; and
- Public interest in disclosure.

Public Interest criteria includes:

- The prevention and detection of crime;
- The prevention / detection of crime and / or apprehension or prosecution of offenders;
- For the exercise of functions necessary for compliance with a legal obligation to which the controller is subject;
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- In accordance with a court order; and
- Common Law Duty of Confidentiality.

When judging public interest the following should be considered:

- Is the intended disclosure proportionate to the intended aim;
- What is the impact of disclosure likely to be on an alleged offender or victim;
- Is there another equally effective means of achieving the same aim;
- Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public;
- Is it necessary to disclose the information to protect an animal; and
- The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

Appendix 6

Secure Handling of PSNI Data

Introduction

i. In line with HM Government mandatory requirements, PSNI has adopted the Government Protective Marking Scheme (GPMS). This scheme requires that a protective marking is applied to all PSNI information assets, e.g. paper documents, email, electronic documents, to ensure that they are protected and managed in a manner proportionate to their importance and sensitivity. The GPMS applies to information assets through their entire lifecycle, i.e. from creation through to secure disposal.

ii. Protective markings are assigned to information assets based on the impact that the compromise of the information asset would bring about. A protective marking must be applied to information assets which, if compromised, may result in certain detrimental outcomes, specifically:

- Increase the risk to life and safety of an individual or a group of individuals;
- Have a detrimental effect on the provision of emergency services;
- Hinder or impede crime fighting; and/or
- Have a negative effect on judicial proceedings.

iii. Failure to assign an appropriate protective marking may lead to data being inadequately protected with subsequent damage, disclosure or loss. Too high an assignment of a protective marking can lead to costly and prohibitive security controls being put in place which may limit the worth of the information asset;

iv. Protectively marked PSNI data shared with councils must be handled as stipulated in the following guidance.

Information Assets Covered

i. The guidance in the following sections covers, but is not limited to, the following types of electronic and paper based information assets:

Table 1 – Asset Types

Information Assets	
○ Assets on electronic media	○ Paper or electronic log files
○ Assets on removable media	○ Paper files
○ CCTV footage	○ Paper forms
○ Dictaphone/sound recordings	○ Photocopied information
○ Digital images	○ Photographic information
○ Electronic documents (e.g. Word & Excel)	○ Hand-written notes
○ Electronic forms	○ Transcribed notes
○ Emails	○ Presentations
○ Film or video	○ Spoken conversations
○ Hard copy documents	○ Speeches or lectures

General Principles

i. In accordance with the HM Government Security Policy Framework Mandatory Requirements user access to PSNI data must be based on the principle of 'least privilege' in combination with the principle of 'need to know'. These principles are defined as:

1) 'Least privilege' – Users must only have access to PSNI Information Assets which are necessary for them to fulfil their role. Users must not have more privileges (access and functionality) than required; and

2) 'Need to know' – User access to PSNI Information Assets must be for specific and legitimate business purposes only.

For the avoidance of doubt, this means that even where a user has been given access to PSNI Information Assets, they must only do so where a genuine business need exists.

ii. The GPMS provides guidance on information asset sensitivity and criticality and the level of suggested protective marking that should be applied. The following table provides guidance on the potential outcome if sensitive, protectively marked data is compromised.

Protective Marking	Information Asset Exposure Could ……
RESTRICTED	• Cause substantial distress to individuals; • Prejudice the investigation or facilitate the commission of crime; • Breach proper undertakings to maintain the confidence of information provided by third parties; • Breach statutory restrictions on disclosure of information.
PROTECT	• Cause distress to individuals; • Breach proper undertakings to maintain the confidence of information provided by third parties; • Breach statutory restrictions on the disclosure of information; • Prejudice the investigation or facilitate the commission of crime; and/or

Guidance for Protectively Marked Information Assets

The following guidance must be applied to the management of protectively marked PSNI information assets, specifically:

i. The originator or Information Asset Owner (IAO) of an information asset is responsible for the correct application of a protective marking.

ii. The protective marking of a PSNI information asset must not be amended without PSNI authority.

iii. Access to protectively marked information must be granted on a 'need to know' basis.

iv. A grouping of information assets must display the protective marking of the highest protectively marked asset. For example, a folder containing five Not Protectively Marked documents and one RESTRICTED document must attract the protective marking of RESTRICTED.

v. Protectively marked information assets must only be accessed by users with an appropriate level of security clearance and where the information being accessed is required for their role.

vi. Where protectively marked information assets are being sent in the post (internal and external) or with courier services, messengers/couriers must be given clear instructions about delivery of items in the absence of the addressee.

vii. Envelopes containing protectively marked information must not be left in vacant rooms, and unopened envelopes should not be left in correspondence trays.

viii. All protectively marked information assets should be accounted for to ensure that they are securely handled and disposed of correctly.

ix. The copying of protectively marked documents should be kept to the minimum essential for the efficient conduct of business. Spare copies should be reviewed regularly with the aim of destruction.

x. Data Protection legislation requires, where information assets relate to individuals, that the information held should be adequate, relevant and not excessive and not kept longer than necessary.

xi. Protectively marked information assets must be secured appropriately when not in use.

xii. Filing cabinets and rooms used for the processing and storage of sensitive information, including back-up disks, video and audio recordings, must be kept locked at all times outside normal working hours.

xiii. Access to protectively marked information outside normal working hours must be controlled and sufficient information of all such access must be recorded to facilitate an audit trail.

xiv. The practice of leaving documents containing protectively marked information in unsecured filing cabinets and rooms, to facilitate easy access at all times, is unacceptable. Managers of protectively marked information must ensure that all filing cabinets etc. are locked at the end of normal working hours. All access keys must be kept under equally secure conditions. In some instances it will be appropriate to document details of the issue of keys to sensitive or secure zones by maintaining a key register; and

xv. A clear desk policy protects information from unauthorised access, loss or damage. All staff should adopt a clear desk policy for papers and diskettes/CDs, to reduce the risks of unauthorised access, loss of and damage to information, outside normal working hours. No matter how good the external security of any office environment, information left on desks is likely to be damaged or destroyed in a disaster (such as fire, flood or explosion). Ideally, fire resistant cabinets should be used for such storage.

Management of Protectively Marked Information Assets

Baseline Security Guidance

i. Any PSNI information asset under the control or custody of ASBF agency must be handled and given a level of protection commensurate with its protective marking. For each protective marking, the baseline security guidance is detailed in the tables below.

Protective Marking Baseline Security Guidance

PROTECT	**Information Asset** • Handle, use and transmit with care; and • Take basic precautions against accidental compromise or opportunist attack. **Physical Asset** • Control, use and transport with care; and • Take basic precautions against accidental compromise or opportunist attack.
RESTRICTED	**Information Asset** • Handle, use and transmit with care; and • Take basic precautions against accidental compromise or opportunist attack. **Physical Asset** • Control, use and transport with care; and • Take basic precautions against accidental compromise or opportunist attack.

Handling and Management of Protectively Marked Information Assets		
Protectively Marked at	**Restricted**	**Protect**
Storage of Physical Assets	Lockable Cabinet	Lockable Cabinet
Can it be emailed externally?	Only between secure domains i.e. • cjsm.net	Yes, controls required for personal data.
Can it be Faxed?	No	Yes, controls required for personal data.
Sending Hard Copy	Trusted hand, post or courier. Closed cover or container. The cover should not be marked other than PERSONAL or ADDRESSEE ONLY. It should be addressed to an individual by name or appointment.	Trusted hand, post or courier. Closed cover or container. The cover should not be marked other than PERSONAL or ADDRESSEE ONLY. It should be addressed to an individual by name or appointment.
Can it be stored on Removable Media?	Only if baseline encryption is used.	Yes, controls required for personal data.